CNUDCI
COMMISSION DES NATIONS UNIES POUR
LE DROIT COMMERCIAL INTERNATIONAL

Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques

NATIONS UNIES

COMMISSION DES NATIONS UNIES POUR LE DROIT COMMERCIAL INTERNATIONAL

Promouvoir la confiance dans le commerce électronique: questions juridiques relatives à l'utilisation internationale des méthodes d'authentification et de signature électroniques

NATIONS UNIES
Vienne, 2009

PUBLICATIONS DES NATIONS UNIES
Numéro de vente: F.09.V.4
ISBN 978-92-1-233467-7

Avant-propos

En 2004, ayant achevé ses travaux relatifs à la Convention sur l'utilisation de communications électroniques dans les contrats internationaux, le Groupe de travail IV (commerce électronique) de la Commission des Nations Unies pour le droit commercial international (CNUDCI) a prié le secrétariat de continuer à suivre diverses questions liées au commerce électronique, notamment celles ayant trait à la reconnaissance transfrontière des signatures électroniques, et de publier les résultats de ses recherches en vue de faire des recommandations à la Commission sur le point de savoir s'il serait possible d'entreprendre des travaux dans ces domaines (voir A/CN.9/571, par. 12).

En 2005, la CNUDCI a pris note des travaux entrepris par d'autres organisations dans divers domaines liés au commerce électronique et a prié le secrétariat de réaliser une étude plus détaillée, qui devrait contenir des propositions sur la forme et la nature d'un document de référence général examinant les divers éléments requis pour créer un cadre juridique favorable au commerce électronique, que la CNUDCI pourrait envisager d'élaborer dans l'avenir afin d'aider les législateurs et les responsables politiques du monde entier[1].

En 2006, la CNUDCI a examiné une note établie par son secrétariat conformément à cette demande (A/CN.9/604). Cette note identifiait les domaines suivants comme éléments possibles d'un document de référence général: *a)* authentification et reconnaissance internationale des signatures électroniques; *b)* responsabilité et normes de conduite pour les fournisseurs d'accès à l´Internet; *c)* facturation électronique et questions juridiques liées aux chaînes logistiques dans le commerce électronique; *d)* transfert de droits sur des biens meubles corporels et d'autres droits par des communications électroniques; *e)* concurrence déloyale et pratiques commerciales trompeuses dans le commerce électronique; et *f)* vie privée et protection des données dans le commerce électronique. La note désignait aussi d'autres questions qui, bien que de façon abrégée, pourraient être traitées dans un tel document: *a)* protection des droits de propriété intellectuelle; *b)* communications électroniques non sollicitées (spams); et *c)* cybercriminalité. Lors de cette session, selon un avis qui a trouvé des appuis, la tâche des législateurs et des responsables politiques, en particulier dans les pays en développement, serait considérablement facilitée si la CNUDCI élaborait un document de référence général traitant des questions mises en évidence par le secrétariat. Un tel document, a-t-on ajouté, pourrait aussi aider la CNUDCI à identifier des domaines dans lesquels elle pourrait entreprendre elle-même des travaux d'harmonisation dans l'avenir. La CNUDCI a demandé à son secrétariat de préparer un spécimen de

[1] *Documents officiels de l'Assemblée générale, soixantième session, supplément n° 17* (A/60/17), paragraphe 214.

chapitre du document de référence général traitant spécifiquement de questions liées à l'authentification et à la reconnaissance internationale des signatures électroniques, pour examen à sa quarantième session, en 2007[2].

Le spécimen de chapitre que le secrétariat a établi pour donner suite à cette demande (A/CN.9/630 et Add.1 à 5) a été présenté à la CNUDCI à sa quarantième session. Celle-ci a félicité le secrétariat d'avoir rédigé ce spécimen de chapitre et lui a demandé de le publier sous la forme d'une publication indépendante[3].

La présente publication analyse les principales questions juridiques découlant de l'utilisation de méthodes de signatures et d'authentification électroniques dans les opérations internationales. La première partie donne un aperçu de l'ensemble de ces méthodes et de leur traitement juridique dans divers pays. La deuxième partie examine l'utilisation de méthodes de signatures et d'authentification dans les opérations internationales et indique les principales questions juridiques liées à leur reconnaissance transfrontière. On a fait observer que, sur le plan international, les difficultés juridiques seront sans doute liées davantage à l'utilisation transfrontière des méthodes de signature et d'authentification électroniques qui demandent l'intervention de tiers dans le processus de signature ou d'authentification. C'est le cas, par exemple, des méthodes s'appuyant sur des certificats émis par un tiers de confiance prestataire de services de certification, en particulier les signatures numériques dans une infrastructure à clef publique. C'est pour cette raison que la deuxième partie de la présente publication consacre une attention toute spéciale à l'utilisation internationale des signatures numériques dans une infrastructure à clef publique. Il ne faudrait pas y voir pour autant l'expression d'une préférence ou d'une prise de position en faveur d'un type particulier de méthode ou de technologie d'authentification.

[2]Ibid., *Soixante et unième session, supplément n° 17* (A/61/17), paragraphe 216.

[3]Ibid., *Soixante-deuxième session, supplément n° 17* (A/62/17), paragraphe 195.

Table des matières

Introduction

1. L'informatique et la technologie de l'information ont mis au point divers moyens pour relier l'information sous forme électronique à des personnes ou à des entités particulières, pour assurer l'intégrité de ces informations ou pour permettre à ces personnes de démontrer qu'elles ont le droit ou l'autorisation d'accéder à un certain service ou à une certaine source d'information. On parle parfois de façon générique, à propos de ces fonctions, de méthodes d'"authentification" électronique ou de "signature" électronique. Parfois, cependant, des distinctions sont faites entre "authentification" électronique et "signature" électronique. L'usage de la terminologie non seulement est incohérent, mais aussi, dans une certaine mesure, source de méprises. Dans un environnement papier, les mots "authentification" et "signature" ainsi que les actions d'"authentifier" et de "signer" n'ont pas exactement la même connotation selon les systèmes juridiques, et ont des fonctionnalités qui ne correspondent pas toujours nécessairement à l'objet et à la fonction de ce que l'on appelle les méthodes d'"authentification" et de "signature" électroniques. De plus, le mot "authentification" est parfois utilisé de manière générique en liaison avec l'assurance à la fois de la qualité d'auteur et de l'intégrité de l'information, mais certains systèmes juridiques peuvent faire une distinction entre ces éléments. Il est donc nécessaire de passer brièvement en revue les différences de terminologie et d'interprétation juridique afin d'établir le champ d'application du présent document.

2. Dans les pays de *common law*, pour la preuve civile, un enregistrement ou un document est considéré comme "authentique" s'il y a la preuve "qu'il est ce que son auteur prétend"[1]. La notion de "document" en tant que telle est très large et englobe généralement "toute chose dans laquelle des informations de toute nature sont enregistrées"[2]. Elle engloberait, par exemple, des choses telles que des photographies de tombes et de maisons[3], des livres comptables[4] et des dessins et plans[5]. On établit la pertinence d'un document comme élément de preuve en le reliant à une personne, à un endroit ou à une chose, processus qui dans certains pays de *common law* est connu sous le nom d'"authentification"[6]. La signature d'un document est un moyen courant – mais non

[1]États-Unis d'Amérique, Federal Rules of Evidence, paragraphe *a)* de l'article 901: ("L'exigence d'authentification ou d'identification comme condition préalable à la recevabilité est satisfaite par un témoignage suffisant pour appuyer la constatation que le contenu du document est ce que prétend son auteur.").

[2]Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, Civil Evidence Act 1995, chapitre 38, section 13.

[3]*Lyell* c. *Kennedy* (nº 3) (1884) 27 Ch.D.1 (Royaume-Uni, Chancery Division).

[4]*Hayes* c. *Brown* [1920] 1 K.B. 250 (Royaume-Uni, Law Reports, King's Bench).

[5]J. H. Tucker & Co., Ltd. c. *Board of Trade* [1955] 2 All ER 522 (Royaume-Uni, All England Law Reports).

[6]*Farm Credit Bank of St. Paul* c. *William G. Huether,* 12 avril 1990 (454 N.W.2d 710, 713) (États-Unis, Supreme Court of North Dakota, North Western Reporter).

exclusif – d'"authentification" et, selon le contexte, les mots "signer" et "authentifier" peuvent être synonymes[7].

3. Une "signature", quant à elle, est "tout nom ou symbole utilisé par une partie avec l'intention d'en faire sa signature"[8]. Il est entendu que l'objet des lois qui exigent qu'un document particulier soit signé par une personne particulière est de confirmer la sincérité du document[9]. L'archétype de la signature est le nom du signataire, écrit de sa propre main, sur un document papier (signature "manuscrite")[10]. Toutefois, la signature manuscrite n'est pas le seul type de signature concevable. Du fait que les tribunaux considèrent les signatures comme "une simple marque", à moins que la loi en question exige qu'elle soit autographe, "le nom imprimé de la partie qui est tenue de signer le document suffit", ou la signature "peut être imprimée sur le document au moyen d'un cachet où est gravé un fac-similé de la signature ordinaire du signataire", à condition que la preuve soit fournie dans de tels cas "que le nom imprimé sur le cachet a été apposé par le signataire", ou que cette signature "a été reconnue et que le signataire a été informé qu'elle avait été faite sous son autorité pour être attachée à l'instrument particulier"[11].

4. Dans les pays de *common law*, c'est généralement dans le "*British Statute of Frauds*" (loi britannique sur les fraudes)[12] et ses versions dans d'autres pays[13] que l'on trouve des prescriptions légales sur la signature comme condition de la validité de certains actes. Avec le temps, les tribunaux ont eu tendance à interpréter cette loi de façon large, en reconnaissant que ses prescriptions rigoureuses concernant la forme avaient été conçues dans des circonstances particulières[14] et que l'observation stricte

---

[7]Dans le contexte de l'article 9 révisé du Code de commerce uniforme des États-Unis, par exemple, "authentifier" est défini comme "A) signer"; ou "B) exécuter ou adopter d'une autre manière un symbole, ou coder ou traiter de façon similaire un enregistrement en totalité ou en partie, avec l'intention présente de la personne authentifiante d'identifier la personne et d'adopter ou d'accepter un enregistrement".

[8]*Alfred E. Weber* c. *Dante De Cecco*, 14 octobre 1948 (1 N.J. Super. 353, 358) (United States, New Jersey Superior Court Reports).

[9]*Lobb* c. *Stanley* (1844), 5 Q.B. 574, 114 E.R. 1366 (Royaume-Uni, Law Reports, Queen's Bench).

[10]Lord Denning in Goodman c. Eban [1954] Q.B.D., 550 à 56: "Dans l'usage anglais moderne, lorsqu'un document doit être signé par une personne, cela signifie que cette personne doit écrire son nom de sa propre main". (Royaume-Uni, Queen's Bench Division).

[11]*R.* c. *Moore: ex parte Myers* (1884) 10 C.L.R., 322 à 324 (Royaume-Uni, Victorian Law Reports).

[12]Le "*Statute of Frauds*" (loi sur les fraudes) a été adopté initialement en Grande-Bretagne en 1677 "pour prévenir de nombreuses pratiques frauduleuses dont on essaie souvent de défendre la validité par faux témoignage ou incitation au faux témoignage". La plupart de ses dispositions ont été abrogées au Royaume-Uni au cours du XX^{e} siècle.

[13]Par exemple, l'article 2-201, alinéa 1 du Code de commerce uniforme des États-Unis, qui a exprimé la loi sur les fraudes comme suit: "Sauf dispositions contraires contenues dans cet article, un contrat de vente de marchandises d'un montant égal ou supérieur à 500 dollars des États-Unis, ne peut être invoqué par voie d'action ou d'exception, à moins qu'il n'existe un écrit suffisant pour prouver qu'un contrat de vente a été conclu entre les parties, signé par la partie contre laquelle l'exécution est demandée, ou par son mandataire ou son courtier".

[14]Le "*Statute of Frauds*" a été adopté en un temps où le législateur était enclin à considérer que les affaires devraient être jugées selon des règles fixes, au lieu de laisser le jury examiner l'effet de la preuve dans chaque cas. Cette conception a sans aucun doute son origine, dans une certaine mesure, dans le fait qu'à cette époque le demandeur et le défendeur n'étaient pas des témoins compétents" (J. Roxborough, dans *Leeman* c. *Stocks* (1951) 1 chapitres 941 à 947-8 (Royaume-Uni, Law Reports, Chancery Division citant l'agrément de l'avis de J. Cave dans *Evans* c. *Hoare* [1892] 1 QB, 593 à 597 (Royaume-Uni, Law Reports, Queen's Bench).

de ses règles risquait inutilement de priver les contrats de leurs effets juridiques[15]. C'est pourquoi, au cours des 150 dernières années, les pays de *common law* ont vu évoluer le concept de "signature", avec un déplacement d'accent de la forme vers la fonction[16]. Des variantes sur ce thème ont été envisagées épisodiquement par les tribunaux anglais, allant de simples modifications telles que croix[17] ou initiales[18], pseudonymes[19] et formules d'identification[20], jusqu'aux noms imprimés[21], à la signature par des tiers[22] et aux tampons en caoutchouc[23]. À chaque fois, les tribunaux ont pu régler la question de la validité de la signature en faisant une analogie avec une signature manuscrite. On pourrait donc dire que dans un contexte caractérisé par des exigences générales de forme rigides, les tribunaux des pays de *common law* ont eu tendance à développer une interprétation assez large des notions d'"authentification" et de "signature", en s'intéressant plus à l'intention des parties qu'à la forme de leurs actes.

5. Les pays de droit romain ont une approche de l'"authentification" et de la "signature" qui diffère à certains égards de celle des pays de *common law*. Ils suivent pour la plupart la règle de la liberté de forme pour les engagements contractuels dans les matières de droit privé, expressément[24] ou implicitement[25], sous réserve toutefois d'un

---

[15]Comme l'a expliqué Lord Bingham of Cornhill, "il est rapidement devenu évident que si la solution adoptée au XVII siècle réglait un problème, elle pouvait en créer un autre, à savoir qu'une partie, concluant sur ce qu'elle pensait être une convention verbale contraignante et agissant en conséquence, voyait ses attentes commerciales déçues quand, au moment de l'exécution, l'autre partie invoquait avec succès l'absence de note ou de mémoire écrit relatifs à la convention" (*Actionstrength Limited* c. *International Glass Engineering*, 3 avril 2003, [2003] UKHL 17) (Royaume-Uni, Chambre des lords).

[16]Chris Reed, "What is a Signature?", *The Journal of Information, Law and Technology*, vol. 3 (2000), et la référence à la jurisprudence qui y figure, accessible sur le site Internet: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed/ (consulté le 5 juin 2008)).

[17]*Baker* c. *Dening* (1838) 8 A. & E. 94 (Royaume-Uni, Adolphus and Ellis' Queen's Bench Reports).

[18]*Hill* c. *Hill* [1947] Ch 231 (Royaume-Uni, Chancery Division).

[19]*Redding, in re* (1850) 14 Jur. 1052, 2 Rob. Ecc. 339 (Royaume-Uni, Jurist Reports and Robertson's Ecclesiastical Reports).

[20]*Cook, In the Estate of (Deceased) Murison* c. *Cook and Another* [1960] 1 All ER 689 (Royaume-Uni, All England Law Reports).

[21]*Brydges* c. *Dicks* (1891) 7 TLR 215 (cité dans *Brennan* c. *Kinjella Pty Ltd*., Supreme Court of New South Wales, 24 juin 1993, 1993 NSW LEXIS 7543, 10). Les documents dactylographiés sont aussi pris en considération dans *Newborne* c. *Sensolid (Great Britain), Ltd*. [1954] 1 QB 45 (Royaume-Uni, Law Reports, Queen's Bench).

[22]*France* c. *Dutton*, 24 avril 1891 [1891] 2 QB 208 (Royaume-Uni, Law Reports, Queen's Bench).

[23]*Goodman* c. *J. Eban Ltd*., [1954] 1 QB 550, cité dans *Lazarus Estates, Ltd*. c. *Beasley*, Court of Appeal, 24 janvier 1956 ([1956] 1 QB 702); *London County Council* c. *Vitamins, Ltd., London County Council* c. *Agricultural Food Products, Ltd*., Court of Appeal, 31 mars 1955 [1955] 2 QB 218 (Royaume-Uni, Law Reports, Queen's Bench).

[24]Cela est reconnu, par exemple, au paragraphe 1 de l'article 11 du Code suisse des obligations. De même, l'article 215 du code civil allemand dispose que les accords ne sont invalidés que lorsqu'ils ne respectent pas une forme prescrite par la loi ou convenue par les parties. Sauf dans de tels cas, il est généralement entendu que les contrats de droit privé ne sont pas soumis à des exigences de forme particulières. Lorsque la loi prescrit expressément une forme particulière, cette exigence doit être interprétée de façon stricte.

[25]En France, par exemple, la liberté de la forme est une conséquence des règles de base applicables à la formation des contrats en vertu du code civil. Selon l'article 1108 du code civil français, la validité d'une convention exige le consentement de la partie qui s'oblige, sa capacité de contracter, un objet certain et une cause licite. Aux termes de l'article 1134, lorsque ces conditions sont remplies, les conventions "tiennent lieu de loi à ceux qui les ont faites". C'est également la règle en Espagne en vertu des articles 1258 et 1278 du code civil espagnol. L'Italie suit elle aussi la même règle, mais de manière moins explicite (voir le code civil italien, articles 1326 et 1350).

catalogue plus ou moins long d'exceptions selon les pays. Cela signifie qu'il n'est pas nécessaire, en règle générale, que les contrats soient "écrits" ou "signés" pour être valides et exécutoires. Certains de ces pays, toutefois, exigent en général un écrit pour prouver le contenu des contrats, sauf en matière commerciale[26]. Contrairement aux pays de *common law*, les pays de droit romain tendent à interpréter les règles de la preuve de manière assez stricte. Le plus souvent, les règles de preuve civile établissent une hiérarchie des preuves pour prouver le contenu des contrats civils et commerciaux. Occupent le rang le plus élevé les documents délivrés par des autorités publiques, suivis par les actes (originaux) sous seing privé. Souvent, cette hiérarchie est conçue de manière que les notions de "document" et de "signature", bien que formellement distinctes, puissent devenir presque indissociables[27]. D'autres pays de droit romain, en revanche, relient de façon positive la notion de "document" à l'existence d'une "signature"[28]. Cela ne signifie pas qu'un document non signé est nécessairement dépourvu de toute valeur probante, mais il ne bénéficiera pas d'une présomption particulière et n'est généralement pas considéré comme un "commencement de preuve"[29]. La plupart des pays de droit romain interprètent le concept d'"authentification" de façon assez étroite, comme signifiant que l'authenticité d'un document a été vérifiée et certifiée par une autorité publique compétente ou un notaire. En procédure civile il est courant de se référer plutôt à la notion d'"originalité" des documents.

6. À l'instar des pays de *common law*, le paradigme de la signature est, dans les pays de droit romain, la signature manuscrite. Certains pays tendent à admettre divers équivalents, y compris des reproductions mécaniques, malgré une approche généralement formaliste de la preuve[30]. D'autres pays, cependant, admettent des signatures mécaniques pour les opérations commerciales[31], mais continuaient, jusqu'à l'avènement des technologies informatiques, à exiger une signature manuscrite pour la preuve d'autres types de contrats[32]. On pourrait donc dire, compte tenu de ce principe général de liberté

---

[26]L'article 1341 du code civil français exige un écrit pour la preuve de contrats excédant une certaine valeur, mais l'article 109 du code de commerce admet divers types de preuve, sans hiérarchie particulière. Cela a conduit la Cour de cassation à reconnaître, en 1892, le principe général de la liberté de la preuve en matière commerciale (Cass. cic. 17 mai 1892, DP 1892.1.604; cité dans Luc Grynbaum, *Preuve, Répertoire de droit commercial,* Dalloz, juin 2002, sect. 6 et 11).

[27]Ainsi, en droit allemand, par exemple, une signature n'est pas un élément essentiel de la notion de "document" (*Urkunde*) (Gerhard Lüke et Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 415, nº 6). Néanmoins, la hiérarchie des preuves documentaires établie par les sections 415, 416 et 419 du code de procédure civile allemand lie clairement la signature au document. En fait, la section 416, sur la valeur probante des actes sous seing privé (*Privaturkunden*) dispose que ces derniers constituent une "preuve complète" pour l'information qu'ils contiennent tant qu'ils sont signés par l'auteur ou par une signature légalisée. Du fait que rien n'est prévu pour les actes sans signature, il semble qu'ils partagent le sort des documents défectueux (c'est-à-dire altérés, endommagés), dont la valeur probante est "établie librement" par les tribunaux (code de procédure civile, section 419).

[28]Ainsi, en France, la signature est un "élément essentiel" des actes sous seing privé (voir Recueil Dalloz, *Preuve*, nº 638).

[29]C'est la situation en France, par exemple, (voir Recueil Dalloz, *Preuve*, nº 657-658).

[30]Les commentateurs du code de procédure civile allemand font observer que l'exigence d'une signature manuscrite reviendrait à exclure toutes les formes de signes obtenus mécaniquement, ce qui irait à l'encontre de la pratique ordinaire et du progrès technologique (voir Gerhard Lüke et Alfred Walchshöfer, *Münchener Kommentar zur Zivilprozessordnung* (Munich, Beck, 1992), section 416, nº 5).

[31]Par exemple, la France (voir Recueil Dalloz, *Preuve*, nº 662).

[32]En France, par exemple, la signature ne pouvait être remplacée par une croix ou d'autres signes, par un sceau ou des empreintes digitales (voir Recueil Dalloz, *Preuve*, nº 665).

de la forme pour les contrats commerciaux, que les pays de droit romano-germanique tendent à appliquer des normes strictes pour évaluer la valeur probante des actes sous seing privé et peuvent faire peu de cas des documents dont l'authenticité n'est pas immédiatement reconnaissable sur le fondement d'une signature.

7. Les considérations ci-dessus montrent non seulement que les notions de signature et d'authentification ne font pas l'objet d'une interprétation uniforme, mais aussi que les fonctions qu'elles remplissent varient selon les systèmes juridiques. Malgré ces divergences, il existe quelques éléments généraux communs. Les notions d'"authentification" et d'"authenticité" sont généralement interprétées en droit comme renvoyant à la sincérité d'un document ou d'un enregistrement, c'est-à-dire que le document est le support "original" des renseignements qu'il contient, sous la forme où il a été enregistré et sans altération. Les signatures, pour leur part, remplissent trois fonctions principales dans l'environnement papier: elles rendent possible l'identification du signataire (fonction d'identification); elles apportent une certitude quant à la participation de cette personne à l'acte de signature (fonction de preuve); et elles associent cette personne à la teneur d'un document (fonction d'attribution). On peut dire des signatures qu'elles remplissent diverses fonctions également, selon la nature du document qui a été signé. Par exemple, une signature pourrait témoigner de l'intention d'une partie d'être liée par la teneur d'un contrat signé; de l'intention d'une personne de revendiquer la paternité d'un texte (montrant ainsi qu'elle a conscience du fait que l'acte de signature peut avoir éventuellement des conséquences juridiques); de l'intention d'une personne de s'associer à la teneur d'un document rédigé par quelqu'un d'autre; et du fait que, et du moment où, une personne se trouvait en un lieu donné[33,34].

8. Il convient toutefois de noter que même si l'authenticité est souvent présumée par l'existence d'une signature, une signature à elle seule n'"authentifie" pas un document. Les deux éléments peuvent même être séparables, selon les circonstances. Une signature peut conserver son "authenticité" même si le document sur lequel elle est apposée est altéré par la suite. De la même façon, un document peut encore être "authentique" alors qu'une signature qu'il contient a été contrefaite. Qui plus est, le pouvoir d'intervenir dans une opération et l'identité réelle de la personne en question, éléments pourtant importants pour assurer l'authenticité d'un document ou d'une signature, ne sont pas entièrement démontrés par la signature seule, et ne sont pas non plus une garantie suffisante de l'authenticité du document ou de la signature.

9. Cette observation débouche sur un autre aspect de la question examinée ici. Quelle que soit la tradition juridique, une signature, à très peu d'exceptions près, ne se suffit pas à elle-même. Son effet juridique dépend du lien entre elle et la personne

---

[33] *Loi type de la CNUDCI sur les signatures électroniques et Guide pour son incorporation, 2001*, (publication des Nations Unies, numéro de vente: F.02.C.8), deuxième partie, paragraphe 29 (accessible sur le site Internet: http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf).

[34] Cette analyse avait déjà servi de base pour les critères de l'équivalence fonctionnelle dans l'article 7 de la *Loi type de la CNUDCI sur le commerce électronique et Guide pour son incorporation, 1996 avec article 5 bis tel qu'ajouté en 1998* (publication des Nations Unies, numéro de vente: F.99.C.4), accessible sur le site Internet: http://www.uncitral.org/pdf/french/texts/electcom/ml-elecsign-f.pdf.

à laquelle elle est attribuable. Dans la pratique, diverses mesures peuvent être prises pour vérifier l'identité du signataire. Lorsque les parties sont toutes présentes au même endroit en même temps, elles peuvent simplement se reconnaître en se voyant; si elles négocient par téléphone, elles peuvent reconnaître leurs voix, etc. Ce sont là des situations courantes qui ne donnent pas lieu à des règles juridiques spécifiques. En revanche, lorsque les parties négocient par correspondance, ou lorsque des documents signés sont expédiés le long d'une chaîne de contrats, il est possible qu'il y ait peu de moyens d'établir que les signes apparaissant sur un document donné y ont bien été apposés par la personne au nom de laquelle ils semblent être liés et de déterminer si seule la personne dûment autorisée a effectivement été celle qui a produit la signature censée lier une personne particulière.

10. Bien qu'une signature manuelle soit une forme familière d'"authentification" et remplisse bien sa fonction pour des documents relatifs à des opérations transmises entre deux parties connues, dans de nombreuses situations commerciales et administratives, une signature est peu sûre. Souvent, la personne qui se fie au document ne connaît pas les noms des personnes autorisées à signer et ne dispose pas non plus de spécimens de signatures à des fins de comparaison[35]. Cela est particulièrement vrai pour de nombreux documents auxquels se fient des pays étrangers dans les opérations commerciales internationales. Même lorsqu'un spécimen de la signature autorisée est disponible à des fins de comparaison, seul un expert peut éventuellement être capable de détecter un faux bien imité. Lorsque de très nombreux documents sont traités, il arrive que les signatures ne soient même pas comparées, sauf pour les opérations les plus importantes. La confiance est l'un des principaux piliers des relations d'affaires internationales.

11. La plupart des systèmes juridiques ont des procédures ou des exigences spéciales destinées à accroître la fiabilité des signatures manuscrites. Certaines procédures peuvent être impératives pour que certains documents produisent des effets juridiques. Elles peuvent aussi être facultatives et à la disposition des parties qui souhaitent agir, de manière à éviter d'éventuelles controverses concernant l'authenticité de certains documents. On peut citer comme exemples typiques:

a) La légalisation. Dans certaines circonstances, l'acte de signature a une importance formelle particulière en raison de la confiance renforcée que l'on associe à une cérémonie spéciale. C'est le cas par exemple avec la légalisation, c'est-à-dire la certification par un notaire afin d'établir l'authenticité d'une signature sur un acte juridique qui, fréquemment, exige la présence physique de la personne devant le notaire;

[35]Certains domaines du droit reconnaissent à la fois l'insécurité inhérente aux signatures manuscrites et l'impossibilité pratique d'insister sur des conditions de forme strictes pour assurer la validité des actes juridiques, et admettent que, dans certains cas, même la falsification d'une signature ne priverait pas un document de son effet juridique. Ainsi, l'article 7 de la Loi uniforme concernant la lettre de change et le billet à ordre, annexée à la Convention portant loi uniforme sur les lettres de change et billets à ordre, conclue à Genève le 7 juin 1930, dispose que "si la lettre de change porte des signatures de personnes incapables de s'obliger par lettre de change, des signatures fausses ou des signatures de personnes imaginaires, ou des signatures qui, pour toute autre raison, ne sauraient obliger les personnes qui ont signé la lettre de change, ou du nom desquelles elle a été signée, les obligations des autres signataires n'en sont pas moins valables". (*Recueil des traités de la Société des Nations,* vol. CXLIII, n° 3313.)

b) L'attestation. L'attestation est l'acte qui consiste à assister à la signature d'un acte juridique puis à signer de son propre nom en tant que témoin. Le but de l'attestation est de conserver la preuve de la signature. En attestant, le témoin déclare et confirme que la personne qu'il a regardée signer l'acte l'a effectivement signé. Attester ne signifie pas se porter garant de l'exactitude ou de la sincérité du document. Le témoin peut être appelé à déposer sur les circonstances entourant la signature[36];

c) Les sceaux. L'utilisation de sceaux, en plus ou à la place de signatures, n'est pas rare, en particulier dans certaines régions du monde[37]. La signature ou l'apposition d'un sceau peuvent, par exemple, prouver l'identité du signataire; que le signataire a accepté d'être lié par l'accord et qu'il l'a fait volontairement; que l'acte est définitif et complet; ou que les renseignements n'ont pas été modifiés après la signature[38]. Elle peut aussi mettre en garde le signataire et indiquer l'intention d'agir d'une manière juridiquement contraignante.

12. En dehors de ces situations spéciales, les signatures manuscrites sont utilisées dans les opérations commerciales, nationales et internationales depuis des siècles, sans cadre législatif ou opérationnel particulier. Les destinataires ou les détenteurs des documents signés ont évalué la fiabilité des signatures au cas par cas en fonction du niveau de confiance dont jouit le signataire. En fait, dans leur grande majorité, les contrats internationaux écrits – si tant est qu'il y ait un "écrit" – ne donnent pas nécessairement lieu à des formalités ou à une procédure d'authentification spéciale.

13. L'utilisation transfrontière de documents signés se complexifie lorsque des autorités publiques interviennent, car les autorités destinataires dans un pays étranger ont généralement besoin de preuves de l'identité et du pouvoir du signataire. Ces exigences sont traditionnellement satisfaites par les procédures dites de "légalisation", où les signatures figurent dans des documents nationaux authentifiés par les autorités diplomatiques, pour être utilisés à l'étranger. Inversement, les représentants consulaires ou diplomatiques du pays dans lequel il est prévu d'utiliser les documents peuvent eux aussi authentifier les signatures d'autorités publiques étrangères dans le pays d'origine. Il est fréquent que les autorités consulaires et diplomatiques n'authentifient que les signatures de certaines autorités de haut rang dans les pays émetteurs, ce qui demande par conséquent plusieurs niveaux de reconnaissance des signatures lorsque le document a été délivré au départ par un agent de rang inférieur, ou bien la légalisation préalable des signatures par un notaire dans le pays émetteur. Dans la plupart des cas, la légalisation est une procédure lourde, longue et coûteuse. C'est pourquoi a été négociée la Convention supprimant l'exigence de la légalisation des actes publics étrangers[39], conclue à La Haye le 5 octobre 1961, afin de remplacer les exigences

[36]Adrian McCullagh, Peter Little et William Caelli, "Electronic signatures: understand the past to develop the future", *University of New South Wales Law Journal*, vol. 21, nº 2 (1998; voir section D du chapitre III sur le concept de témoin).

[37]On utilise des sceaux dans plusieurs pays d'Asie orientale, comme la Chine et le Japon.

[38]Mark Sneddon, "Legislating to facilitate electronic signatures and records: exceptions, standards and the impact of the statute book", *University of New South Wales Law Journal*, vol. 21, nº 2 (1998; voir chapitre II de la deuxième partie, "Policy objectives of writing and signature requirements").

[39]Nations Unies, *Recueil des Traités*, vol. 527, nº 7625.

existantes par un formulaire simplifié et normalisé (l'"apostille"), qui est utilisé pour fournir une certification de certains actes publics dans les États Parties à la convention[40]. Seule une autorité compétente désignée par l'État dont émane l'acte public peut délivrer une apostille. Les apostilles attestent la véracité de la signature, la qualité en laquelle le signataire de l'acte a agi et, le cas échéant, l'identité du sceau ou timbre dont cet acte est revêtu, mais ne concernent pas la teneur de l'acte lui-même.

14. Comme il a été indiqué ci-dessus, dans de nombreux systèmes juridiques, il n'est pas toujours nécessaire que les contrats commerciaux figurent dans un document ou soient attestés par un écrit pour être valables. Même lorsqu'un écrit existe, une signature n'est pas nécessairement impérative pour que le contrat soit contraignant pour les parties. Naturellement, lorsque la loi exige qu'un contrat soit écrit et signé, le non-respect de ces conditions l'invaliderait. Les conditions de forme à des fins de preuve sont peut-être plus importantes que les conditions de forme à des fins de validité des contrats. La difficulté de prouver les conventions verbales est une des principales raisons pour lesquelles les contrats commerciaux sont reproduits dans des documents écrits ou établis par correspondance, même si une convention verbale serait autrement valable. Les parties dont les obligations sont établies dans des écrits signés ont peu de chances de réussir dans les tentatives de contester la teneur de leurs obligations. Des règles strictes sur les preuves documentaires visent généralement à accorder un degré élevé de fiabilité aux documents qui y satisfont, ce qui, estime-t-on généralement, accroît la sécurité juridique. En même temps, cependant, plus les conditions en matière de preuve sont élaborées, plus grande est la possibilité pour une partie d'invoquer des vices de forme pour invalider ou refuser la force exécutoire d'obligations qu'elle n'a plus l'intention d'exécuter, par exemple parce que le contrat est devenu commercialement désavantageux. Il faut donc trouver un équilibre entre l'intérêt de promouvoir la sécurité dans l'échange de communications électroniques et le risque de donner un moyen facile aux négociants de mauvaise foi de refuser d'honorer leurs obligations juridiques librement assumées. Y parvenir par des règles et des normes internationalement reconnues et applicables dans différents pays est une tâche importante pour les décideurs dans le domaine du commerce électronique. L'objet du présent rapport est d'aider les législateurs et les décideurs à identifier les principales questions juridiques en cause dans l'utilisation internationale de méthodes d'authentification et de signature électroniques et d'envisager des solutions possibles.

[40]Ces actes comprennent: les documents qui émanent d'une autorité ou d'un fonctionnaire relevant d'une juridiction de l'État (y compris ceux qui émanent d'un tribunal administratif, constitutionnel ou ecclésiastique, du ministère public, d'un greffier ou d'un huissier de justice); les documents administratifs; les actes notariés; et les déclarations officielles apposées sur un acte sous seing privé.

Première partie

Méthodes de signature et d'authentification électroniques

Table des matières

I. Définition et méthodes de signature et d'authentification électroniques

A. Remarques générales sur la terminologie

15. Les termes "authentification électronique" et "signature électronique" désignent diverses techniques actuellement disponibles sur le marché ou encore en développement pour reproduire dans un environnement électronique certaines ou la totalité des fonctions identifiées comme caractéristiques des signatures manuscrites ou d'autres méthodes traditionnelles d'authentification.

16. Diverses méthodes de signature électronique ont été mises au point au fil des années. Chacune vise à satisfaire des besoins différents et à conférer des niveaux de sécurité différents, et donne lieu à des exigences techniques différentes. Les méthodes d'authentification et de signature électroniques peuvent être classées en trois catégories: celles qui sont fondées sur la connaissance de l'utilisateur ou du destinataire (par exemple, mot de passe, numéro d'identification personnel), celles qui sont fondées sur les caractéristiques physiques de l'utilisateur (par exemple, la biométrie) et celles qui sont fondées sur la possession d'un objet par l'utilisateur (par exemple, codes ou autres renseignements stockés sur une carte magnétique)[41]. On pourrait envisager une quatrième catégorie, comprenant divers types de méthodes qui, sans ressortir à l'une quelconque des catégories précédentes, pourrait aussi être utilisée pour désigner l'auteur d'une communication électronique (comme le fac-similé d'une signature manuscrite, ou un nom dactylographié au bas d'un message électronique). Les technologies actuellement utilisées comprennent: les signatures numériques dans le cadre d'une infrastructure à clef publique (ICP), les dispositifs biométriques, les numéros d'identification personnels (PIN), les mots de passe définis par l'utilisateur ou attribués, les signatures manuscrites scannées, la signature au moyen d'un stylo numérique, et le fait de cliquer sur une case "OK" ou "J'accepte"[42]. Des solutions hybrides fondées sur une combinaison de différentes technologies se répandent de plus en plus, comme c'est le cas, par exemple, avec l'utilisation combinée de mots de passe et des protocoles TLS/SSL (*transport layer security/secure socket layer*), qui est une technologie mêlant chiffrement à clef publique et à clef symétrique. Les caractéristiques des principales techniques actuellement en usage sont décrites ci-dessous (voir paragraphes 25 à 66).

---

[41] Voir le rapport du Groupe de travail sur le commerce électronique sur les travaux de sa trente-deuxième session, tenue à Vienne du 19 au 30 janvier 1998 (A/CN.9/446, paragraphes 91 sq.

[42] *Loi type de la CNUDCI sur les signatures électroniques* …, paragraphe 33 de la deuxième partie.

17. Comme c'est souvent le cas, la technologie s'est développée bien avant que la loi s'intéresse au sujet. Il en résulte un écart, qui entraîne non seulement des niveaux variables de connaissance des experts, mais aussi des incohérences sur l'utilisation la terminologie. Des expressions qui étaient traditionnellement employées avec une connotation particulière dans les droits nationaux ont commencé à être utilisées pour décrire des techniques électroniques dont la fonctionnalité ne coïncidait pas nécessairement avec les fonctions ou caractéristiques du concept correspondant dans l'usage juridique. Comme on l'a vu ci-dessus (voir paragraphes 7 à 10), les notions d'"authentification", d'"authenticité", de "signature" et d'"identité", bien qu'elles soient étroitement liées dans certains contextes, ne sont pas identiques ou interchangeables. Leur usage dans le secteur de la technologie de l'information, qui s'est constitué pour l'essentiel autour des considérations de sécurité des réseaux, ne s'applique pas nécessairement aux mêmes catégories que dans les écrits juridiques.

18. Dans certains cas, l'expression "authentification électronique" désigne des techniques qui, selon le contexte dans lequel elles sont utilisées, peuvent comporter divers éléments tels que l'identification d'individus, la confirmation du pouvoir d'une personne (généralement d'agir au nom d'une autre personne ou entité) ou des prérogatives (par exemple, l'appartenance à une institution ou l'abonnement à un service) ou l'assurance de l'intégrité de l'information. Dans d'autres cas, l'accent est mis sur la seule identité[43], mais il s'étend parfois au pouvoir[44], ou à une combinaison de plusieurs de ces éléments[45].

19. Ni la Loi type de la CNUDCI sur le commerce électronique[46] ni la Loi type de la CNUDCI sur les signatures électroniques[47] n'emploient le terme "authentification électronique", en raison du sens différent du mot "authentification" dans divers systèmes juridiques et de la confusion possible avec des procédures ou des exigences de forme

[43]Le bureau de la Technologie (Technology Administration) du ministère du Commerce des États-Unis, par exemple, définit l'authentification électronique comme "le processus consistant à établir la confiance dans les identités des utilisateurs présentées dans un système d'information" (ministère du Commerce des États-Unis, *Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology,* NIST Special Publication 800-63, version 1.0.2 (Gaithersburg, Maryland, avril 2006), accessible sur le site Internet: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf (consulté le 5 juin 2008)).

[44]Par exemple, le Gouvernement australien a mis au point un cadre d'authentification électronique qui définit celle-ci comme "le processus consistant à établir un niveau de confiance sur le point de savoir si une déclaration est sincère ou valide lors d'une transaction s'effectuant en ligne ou par téléphone. Il aide à renforcer la confiance dans une transaction en ligne en donnant aux parties concernées une certaine assurance que leurs rapports sont légitimes. Ces déclarations peuvent comprendre: des détails sur l'identité; les qualifications professionnelles, ou la délégation de pouvoir pour mener la transaction" (Australie, Department of Finance and Administration, *Australian Government e-Authentication Framework: An Overview* (Commonwealth of Australia, 2005), accessible sur le site Internet: (http://www.agimo.goc.au/infrastructure/authentication/agaf_b/overview/ introduction#e-authentication (consulté le 5 juin 2008)).

[45]Les Principes d'authentification électroniques élaborés par le Gouvernement du Canada, par exemple, définissent l'authentification comme un "processus qui atteste des attributs des parties prenantes à une communication électronique ou de l'intégrité de la communication". Le terme attributs est défini à son tour comme une "information concernant l'identité, les privilèges ou les droits d'une partie prenante ou d'une autre entité identifiée" (Canada, Industrie Canada, *Principes d'authentification électronique – Cadre canadien*, mai 2004, accessible sur le site Internet: http://strategis.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/gv00242f.html (consulté le 5 juin 2008))

[46]*Loi type de la CNUDCI sur le commerce électronique ...* .

[47]*Loi type de la CNUDCI sur les signatures électroniques...* .

particulières. La Loi type sur le commerce électronique utilise à la place la notion de "forme originale" comme critère de l'équivalence fonctionnelle de l'information électronique "authentique". D'après son article 8, lorsque la loi exige qu'une information soit présentée ou conservée sous sa forme originale, un message de données satisfait à cette exigence:

a) "S'il existe "une garantie fiable quant à l'intégrité de l'information à compter du moment où elle a été créée pour la première fois sous sa forme définitive en tant que message de données ou autre"; et

b) Si, lorsqu'il est exigé qu'une information soit présentée, cette information "peut être montrée à la personne à laquelle elle doit être présentée".

20. En conformité avec la distinction faite dans la plupart des systèmes juridiques entre signature (ou sceaux, lorsqu'ils sont utilisés à sa place) comme moyen d'"authentification", d'une part, et "authenticité" en tant que qualité d'un document ou enregistrement, d'autre part, les deux lois types complètent la notion d'"originalité" par celle de "signature". L'alinéa *a)* de l'article 2 de la Loi type de la CNUDCI sur les signatures électroniques définit la signature électronique comme des données sous forme électronique contenues dans un message de données ou logiquement associées audit message, pouvant être utilisées pour "identifier le signataire" dans le cadre du message de données et "indiquer qu'il approuve l'information qui y est contenue".

21. Dans les textes de la CNUDCI, la définition de l'expression "signature électronique" est délibérément large, de manière à englober toutes les méthodes de "signature électronique" existantes et futures. Tant que la fiabilité des méthodes utilisées est "suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris de tout accord en la matière"[48], elles devraient être considérées comme satisfaisant aux prescriptions légales en matière de signature. Les textes de la CNUDCI relatifs au commerce électronique, ainsi que beaucoup d'autres textes législatifs, reposent sur le principe de la neutralité technologique et visent par conséquent à prendre en compte toutes les formes de signature électronique. Ainsi, la définition que la CNUDCI donne de la "signature électronique" couvrirait l'ensemble des techniques de "signature électronique", de la sécurité de haut niveau, telle que les systèmes de garantie de la signature fondés sur la cryptographie associés à une infrastructure à clef publique [forme courante de "signature numérique" (voir paragraphes 25 à 53)] aux niveaux inférieurs, tels que les codes ou mots de passe non chiffrés. La simple dactylographie du nom de l'auteur à la fin d'un message électronique, qui est la forme la plus courante de "signature" électronique, par exemple, remplirait la fonction consistant à identifier correctement l'auteur du message toutes les fois qu'il n'est pas déraisonnable d'appliquer un niveau de sécurité aussi bas.

22. Les lois types de la CNUDCI n'abordent pas autrement les questions liées au contrôle de l'accès ou à la vérification de l'identité. Cela tient aussi au fait que, dans

[48] *Loi type de la CNUDCI sur le commerce électronique* ... alinéa *b)* du paragraphe 1 de l'article 7.

un environnement papier, si les signatures peuvent être des signes de l'identité, elles sont nécessairement attributives de l'identité. La Loi type de la CNUDCI sur le commerce électronique traite toutefois des conditions dans lesquelles le destinataire d'un message de données est fondé à supposer que le message émanait effectivement de son expéditeur présumé. De fait, son article 13 prévoit qu'en ce qui concerne la relation entre l'expéditeur et le destinataire, un message de données est réputé émaner de l'expéditeur s'il a été envoyé par une personne "autorisée à agir à cet effet au nom de l'expéditeur" ou par un "système d'information programmé par l'expéditeur ou en son nom pour fonctionner automatiquement". S'agissant de la relation entre l'expéditeur et le destinataire, ce dernier est fondé à considérer qu'un message de données émane de l'expéditeur et à agir en conséquence *a)* si, pour s'assurer que le message de données émanait de l'expéditeur, il a "correctement appliqué une procédure que l'expéditeur avait précédemment acceptée à cette fin" ou *b)* si le message de données tel qu'il l'a reçu résulte des actes d'une personne qui, de par ses relations avec l'expéditeur ou un agent de celui-ci, a eu accès à une méthode que l'expéditeur utilise pour identifier les messages de données comme étant de lui. Dans l'ensemble, ces règles permettent à une partie de déduire l'identité de quelqu'un d'autre, que le message ait été ou non "signé" électroniquement et que la méthode utilisée pour l'attribuer à l'expéditeur ait été ou non utilisée valablement à des fins de "signature". Cela est conforme à la pratique actuelle dans l'environnement papier. Vérifier la voix, l'apparence physique ou les papiers d'identité (par exemple, un passeport national) d'une personne peut suffire pour conclure que cette personne est celle qu'elle prétend être aux fins de communication avec celle-ci, mais ne tiendrait pas lieu de "signature" de cette personne dans la plupart des systèmes juridiques.

23. Outre la confusion due au fait que les usages technique et juridique des termes dans l'environnement papier et dans l'environnement électronique ne coïncident pas, les diverses techniques mentionnées précédemment (voir le paragraphe 16 ci-dessus et l'analyse plus détaillée aux paragraphes 24 à 66 ci-dessous) peuvent être utilisées à différentes fins et fournir une fonctionnalité différente, selon le contexte. Des mots de passe ou des codes, par exemple, peuvent être utilisés pour "signer" un document électronique mais aussi pour accéder à un réseau, à une base de données ou à un autre service électronique, de façon très ressemblante à une clef dont on se sert pour déverrouiller un coffre ou ouvrir une porte. Toutefois, alors que dans le premier cas le mot de passe est une preuve d'identité, dans le second c'est un certificat *(credential)*, une marque d'autorité qui, bien que lié d'ordinaire à une personne particulière, peut également être transféré à une autre. Dans le cas des signatures numériques, l'inadéquation de la terminologie actuelle est encore plus patente. La signature numérique est largement considérée comme une technologie particulière pour "signer" des documents électroniques. Il n'est toutefois pas du tout certain que l'on puisse, d'un point de vue juridique, dire de l'application de la cryptographie asymétrique à des fins d'authentification qu'elle est une "signature" numérique, car ses fonctions vont au-delà des fonctions typiques d'une signature manuscrite. La signature numérique offre le moyen à la fois de "vérifier l'authenticité de messages électroniques" et de "garantir l'intégrité du contenu". En outre, la technologie de la signature numérique n'établit pas simplement l'origine ou l'intégrité pour ce qui est des individus, comme cela est exigé à des fins de signature, mais elle peut aussi authentifier, par exemple, des serveurs, des sites

Web, des logiciels informatiques, ou toutes autres données distribuées ou stockées numériquement, ce qui confère aux signatures numériques une utilisation beaucoup plus vaste qu'un substitut électronique aux signatures manuscrites[49].

B. Principales méthodes d'authentification et de signature électroniques

24. Aux fins du présent document, quatre méthodes principales d'authentification et de signature électroniques seront examinées: les signatures numériques; les méthodes biométriques; les mots de passe et les méthodes hybrides; les signatures scannées ou saisies au clavier.

1. Signatures numériques fondées sur la cryptographie à clef publique

25. La "signature numérique" désigne des applications technologiques qui utilisent la cryptographie asymétrique, autrement dit un système de chiffrement à clef publique, pour garantir l'authenticité de messages électroniques et l'intégrité de leur contenu. La signature numérique peut prendre de multiples formes, telles que la signature avec arrêt sur défaillance, la signature aveugle et la signature indéniable.

a) Notions techniques et terminologie

i) *Cryptographie*

26. Les signatures numériques sont créées et vérifiées grâce à la cryptographie, branche des mathématiques appliquées, qui s'occupe de la transformation de messages en des formes apparemment inintelligibles et de leur restitution dans leur forme initiale. Les signatures numériques utilisent ce que l'on appelle la "cryptographie à clef publique", qui est souvent basée sur l'utilisation de fonctions algorithmiques pour créer deux "clefs" (c'est-à-dire des grands nombres générés à l'aide d'une série de formules mathématiques appliquées à des nombres premiers) différentes mais mathématiquement liées entre elles[50]. Une clef est utilisée pour créer une signature numérique ou pour transformer des données en une forme apparemment inintelligible, et l'autre

[49]Babette Aalberts et Simone van der Hof, *Digital Signature Blindness: Analysis of Legislative Approaches toward Electronic Authentication* (novembre 1999), page 8, accessible sur le site Internet: http://rechten.uvt.nl/simone/Digsigbl.pdf (consulté le 5 juin 2008).

[50]On notera cependant que le concept de cryptographie à clef publique, tel qu'il est examiné ici, ne nécessite pas forcément l'utilisation d'algorithmes fondés sur des nombres premiers. On utilise ou l'on met au point actuellement d'autres techniques mathématiques telles que des systèmes de cryptographie fondés sur des courbes elliptiques, souvent décrits comme offrant un niveau élevé de sécurité grâce à l'utilisation de longueurs de clefs considérablement réduites.

pour vérifier une signature numérique ou restituer le message dans sa forme initiale[51]. Le matériel et le logiciel informatiques utilisant deux clefs de ce type sont souvent appelés collectivement "cryptosystèmes" ou, plus précisément, "cryptosystèmes asymétriques" lorsqu'ils utilisent des algorithmes asymétriques.

ii) *Clefs publiques et privées*

27. Une clef complémentaire utilisée pour les signatures numériques est appelée "clef privée", n'est utilisée que par le signataire pour créer la signature numérique et doit être tenue secrète, tandis que la "clef publique" est d'ordinaire plus largement connue et est utilisée par une partie qui lui fait confiance pour vérifier la signature numérique. La clef privée est normalement conservée sur une carte à mémoire, ou est accessible grâce à un numéro d'identification personnel (NIP) ou grâce à un dispositif d'identification biométrique, par exemple un dispositif de reconnaissance d'empreinte de pouce. Si plusieurs personnes ont besoin de vérifier la signature numérique du signataire, il faut rendre la clef publique accessible ou la distribuer à chacune de ces personnes, par exemple en attachant les certificats à la signature, ou par d'autres moyens permettant de s'assurer que les parties concernées, et uniquement celles qui ont à vérifier les signatures, ont accès aux certificats correspondants. Bien que les clefs de la paire soient mathématiquement liées, si un système de cryptographie asymétrique a été conçu et mis en œuvre de façon sécurisée, il est pratiquement impossible, connaissant la clef publique, de déduire la clef privée. Les algorithmes les plus courants de chiffrement par utilisation de clefs publiques et privées reposent sur une caractéristique importante des grands nombres premiers: une fois multipliés ensemble pour produire un nouveau nombre, il est particulièrement difficile et long de déterminer les deux nombres premiers qui ont créé ce nouveau nombre plus important[52]. Ainsi, bien que de nombreuses personnes connaissent la clef publique d'un signataire donné et l'utilisent pour vérifier sa signature, elles ne peuvent découvrir la clef privée de ce signataire et l'utiliser pour falsifier des signatures numériques.

---

[51]Bien que le recours à la cryptographie soit l'une des principales caractéristiques des signatures numériques, le simple fait qu'une signature numérique soit utilisée pour authentifier un message contenant des données sous forme numérique ne doit pas être assimilé à l'utilisation plus générale de la cryptographie à des fins de confidentialité. Le codage pour raison de confidentialité est une méthode utilisée pour coder une communication électronique de manière que seuls l'initiateur et le destinataire du message seront en mesure de le lire. Dans un certain nombre de pays, la loi restreint l'utilisation de la cryptographie à cette fin pour des raisons d'ordre public qui peuvent comporter des considérations de défense nationale. Cependant, l'utilisation de la cryptographie aux fins d'authentification par la création d'une signature numérique n'implique pas nécessairement le recours au codage pour garantir le caractère confidentiel d'une communication, étant donné que la signature numérique codée peut être tout simplement jointe à un message non codé.

[52]Certaines normes existantes contiennent la notion d'"infaisabilité informatique" pour décrire l'irréversibilité escomptée du processus, c'est-à-dire l'espoir qu'il sera impossible de déduire la clef privée secrète d'un utilisateur à partir de sa clef publique. "La notion d'"infaisabilité informatique" est un concept relatif fondé sur la valeur des données protégées, l'infrastructure informatique requise pour les protéger, le temps nécessaire pour les protéger, ainsi que le coût et le temps nécessaires pour attaquer les données, ces facteurs étant évalués tant en fonction de la situation actuelle que des futurs progrès technologiques". [American Bar Association, *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce* (Chicago, Association du barreau américain, 1er août 1996), page 9, note 23, accessible sur le site Internet: http://www.abanet.org/scitech/ec/isc/dsgfree.html (consulté le 4 juin 2008)].

iii) *Fonction de hachage*

28. Outre la production de paires de clefs, un autre processus fondamental, généralement appelé "fonction de hachage", est utilisé à la fois pour créer et pour vérifier une signature numérique. Une fonction de hachage est un processus mathématique fondé sur un algorithme, qui crée une représentation numérique, ou forme comprimée du message (souvent appelée "abrégé" ou "empreinte digitale" du message), et qui prend la forme d'une "valeur de hachage" ou d'un "résultat de hachage" d'une longueur normalisée, généralement bien plus courte que le message lui-même, mais qui lui est néanmoins propre. Toute modification apportée au message produit inévitablement un résultat de hachage différent lorsqu'on utilise la même fonction de hachage. Dans le cas d'une fonction de hachage sécurisée, parfois appelée "fonction de hachage unidirectionnelle", il est pratiquement impossible, connaissant la valeur de hachage, de déduire le message initial. Une autre caractéristique fondamentale des fonctions de hachage est qu'il est également pratiquement impossible de trouver un autre objet binaire (c'est-à-dire différent de celui qui a produit l'abrégé à l'origine) qui produira le même abrégé. Les fonctions de hachage permettent donc au programme de création de signatures numériques d'opérer sur des volumes de données limités et plus prévisibles tout en établissant une solide corrélation avec la teneur du message initial, ce qui lui permet d'assurer qu'aucune modification n'a été apportée au message depuis que ce dernier a été signé sous forme numérique.

iv) *Créer une signature numérique*

29. Pour signer un document ou toute autre information, le signataire commence par définir précisément les limites de ce qu'il doit signer. Ensuite, une fonction de hachage opérant dans le programme du signataire calcule un résultat de hachage propre (à toutes fins pratiques) à l'information qui doit être signée. Le programme du signataire transforme ensuite le résultat de hachage en une signature numérique à l'aide de la clef privée du signataire. La signature numérique résultante est par conséquent propre à la fois à l'information signée et à la clef privée utilisée pour créer la signature numérique. Généralement, une signature numérique (chiffrement, avec la clef privée du signataire, du résultat de hachage du message) est attachée au message et stockée ou transmise avec ce message. Cependant, elle peut également être envoyée ou stockée comme élément de données distinct, aussi longtemps qu'elle maintient une association fiable avec le message correspondant. Étant donné qu'une signature numérique est propre à son message, elle est inutilisable si on la dissocie de façon permanente dudit message.

v) *Vérification de la signature numérique*

30. La vérification de la signature numérique consiste à vérifier la signature numérique par rapport au message initial et à une clef publique donnée, et à déterminer de cette façon si la signature numérique a été créée pour ce même message à l'aide de la clef privée correspondant à la clef publique référencée. La vérification

d'une signature numérique s'effectue en calculant un nouveau résultat de hachage du message initial au moyen de la fonction de hachage utilisée pour créer la signature numérique. Ensuite, à l'aide de la clef publique et du nouveau résultat de hachage, le contrôleur vérifie si la signature numérique a été créée à l'aide de la clef privée correspondante et si le résultat de hachage nouvellement calculé correspond au résultat de hachage initial qui a été transformé en signature numérique au cours du processus de signature.

31. Le programme de vérification confirmera que la signature numérique est "vérifiée" du point de vue cryptographique: *a)* si la clef privée du signataire a été utilisée pour signer numériquement le message, ce qui est avéré si la clef publique du signataire a été utilisée pour vérifier la signature, étant donné que la clef publique du signataire permettra de vérifier uniquement une signature numérique créée à l'aide de la clef privée du signataire; et *b)* si le message ne subit aucune modification, ce qui est avéré si le résultat de hachage calculé par la personne chargée de la vérification est identique au résultat de hachage extrait de la signature numérique lors du processus de vérification.

vi) Autres utilisations de la technologie des signatures numériques

32. L'utilisation de la technologie des signatures numériques va bien au-delà de la simple "signature" de communications électroniques à la façon des signatures manuscrites utilisées pour signer des documents. Ainsi, des certificats signés numériquement sont souvent utilisés, par exemple, pour "authentifier" des serveurs ou des sites Internet, afin de garantir à leurs utilisateurs que le serveur ou le site en question est bien celui qu'il prétend être ou est véritablement relié à la société qui prétend le gérer. Cette technologie peut aussi être utilisée pour "authentifier" des logiciels informatiques, par exemple pour garantir l'authenticité du logiciel téléchargé d'un site Internet, ou qu'un serveur donné utilise une technologie largement reconnue comme offrant un certain niveau de sécurité de connexion, ou pour "authentifier" toute autre donnée qui est diffusée ou conservée sous forme numérique.

b) Infrastructure à clef publique et prestataires de services de certification

33. Pour vérifier une signature numérique, le vérificateur doit avoir accès à la clef publique du signataire et être certain que celle-ci correspond bien à la clef privée de ce dernier. Cependant, une paire de clefs publique et privée ne présente aucune association intrinsèque avec une personne quelconque; il s'agit simplement d'une paire de nombres. Un mécanisme supplémentaire est nécessaire pour associer de manière fiable une personne ou une entité particulière à la paire de clefs. Cela est très important car il se peut qu'il n'y ait aucune relation de confiance préexistante entre le signataire et les destinataires de communications signées numériquement. Pour ce faire, les parties concernées doivent avoir confiance dans les clefs publiques et privées émises.

34. Le degré de confiance requis peut exister entre deux parties qui se font confiance, qui ont traité l'une avec l'autre sur une certaine durée, qui communiquent sur des systèmes fermés, qui fonctionnent à l'intérieur d'un groupe fermé, ou dont les relations sont régies par contrat, par exemple dans le cadre d'un accord entre partenaires commerciaux. Si une transaction ne fait intervenir que deux parties, chaque partie peut simplement communiquer (par un moyen relativement sûr tel qu'un coursier ou le téléphone) la clef publique de la paire de clefs que chaque partie va utiliser. Cependant, il se peut que le même degré de confiance soit absent lorsque les parties ont eu peu à faire l'une avec l'autre, communiquent sur des systèmes ouverts (par exemple Internet), ne font pas partie d'un groupe fermé, n'ont pas conclu d'accord de partenariat commercial, ou lorsque leur relation n'est pas régie par un droit particulier. De plus, il faudrait tenir compte du fait que, si des différends doivent être réglés par un tribunal ou par arbitrage, il pourrait être difficile de prouver qu'une certaine clef publique avait, ou n'avait pas, été effectivement donnée au destinataire par son propriétaire légitime.

35. Un signataire éventuel pourrait faire une déclaration publique indiquant que les signatures vérifiables au moyen d'une clef publique donnée devraient être considérées comme provenant de lui. La forme et l'efficacité juridique d'une telle déclaration seraient régies par la loi de l'État adoptant. Par exemple, une présomption d'attribution de signatures électroniques à un signataire particulier pourrait être établie par la publication de la déclaration dans un journal officiel ou dans un document reconnu comme "authentique" par les autorités publiques. Cependant, d'autres parties pourraient refuser d'accepter cette déclaration, en particulier lorsqu'il n'existe aucun contrat préalable établissant avec certitude l'effet juridique de ladite déclaration. Une partie se fiant à une telle déclaration non étayée mais publiée dans un système ouvert courrait alors un risque important de faire confiance, à son insu, à un imposteur, ou d'avoir à établir qu'il n'y a pas eu refus de signature numérique (question souvent évoquée à propos de la "non-révocation" des signatures numériques) dans les cas où une transaction s'avérerait défavorable pour le signataire supposé.

36. Une solution à certains de ces problèmes consiste à recourir à un ou plusieurs tiers de confiance pour associer un signataire identifié ou le nom de ce signataire à une clef publique spécifique. Ce tiers est généralement appelé, dans la plupart des normes et directives techniques "autorité de certification" ou "prestataire de services de certification" (dans la Loi type de la CNUDCI sur les signatures électroniques, c'est l'expression "prestataire de services de certification" qui a été retenue). Dans plusieurs pays, ces autorités de certification s'organisent de façon hiérarchique en ce que l'on appelle souvent une "infrastructure à clef publique" (ICP). Les autorités de certification appartenant à une infrastructure à clef publique peuvent être organisées en une structure hiérarchique dans laquelle certaines autorités de certification ne font qu'en certifier d'autres, qui fournissent directement des services aux utilisateurs. Dans une telle structure, certaines autorités de certification sont donc subordonnées à d'autres. On peut aussi concevoir des structures dans lesquelles toutes les autorités de certification sont sur un pied d'égalité. Dans une grande ICP, il est probable qu'il y aura à la fois des autorités de certification subordonnées et supérieures. D'autres solutions comprennent, par exemple, les certificats délivrés par les parties se fiant à la signature.

i) *Infrastructure à clef publique*

37. Créer une infrastructure à clef publique est un moyen d'inspirer confiance dans le fait que: *a)* la clef publique de l'utilisateur n'a pas été falsifiée et correspond effectivement à sa clef privée; *b)* les techniques de cryptologie utilisées sont fiables. Pour inspirer confiance, une ICP peut offrir un certain nombre de services, dont les suivants: *a)* gérer les clefs cryptographiques utilisées pour les signatures numériques; *b)* certifier qu'une clef publique correspond bien à une clef privée; *c)* fournir des clefs aux utilisateurs finaux; *d)* publier des informations sur la révocation des clefs publiques ou des certificats; *e)* gérer des objets personnalisés (par exemple des cartes à puce) capables d'identifier l'utilisateur au moyen d'éléments d'identification qui lui sont spécifiques ou capables de créer et de garder en mémoire les clefs privées d'un individu; *f)* vérifier l'identité des utilisateurs finaux et leur offrir des services; *g)* offrir des services d'horodatage; et *h)* gérer les clefs cryptographiques utilisées pour le chiffrement de confidentialité lorsque le recours à cette technique est autorisé.

38. Une ICP peut s'appuyer sur divers niveaux hiérarchiques d'autorité. Par exemple, les modèles envisagés dans certains pays pour établir ce type d'infrastructure se réfèrent notamment aux niveaux suivants: *a)* une autorité principale ("autorité source") unique, qui certifierait la technologie et les pratiques de toutes les parties autorisées à produire les paires de clefs cryptographiques ou les certificats concernant l'utilisation de ces paires de clefs, et qui enregistrerait les autorités de certification inférieures[53]; *b)* diverses autorités de certification, situées en dessous de l'autorité source, qui certifieraient que la clef publique d'un utilisateur correspond effectivement à sa clef privée (autrement dit, que la clef n'a pas été manipulée); et *c)* diverses autorités locales d'enregistrement, placées en dessous des autorités de certification, qui recevraient les demandes de paires de clefs cryptographiques ou de certificats relatifs à l'utilisation de ces paires de clefs adressées par des utilisateurs, autorités qui exigeraient une preuve d'identification et vérifieraient l'identité des utilisateurs éventuels. Dans certains pays, il est envisagé de confier à des notaires la fonction d'autorité locale d'enregistrement, ou tout au moins de leur demander d'apporter leur concours à cette fonction.

39. Les infrastructures à clef publique structurées de manière hiérarchique sont modulables, en ce sens qu'elles peuvent incorporer de nouvelles "communautés" d'ICP entières en chargeant simplement leur autorité source d'établir une relation de confiance avec une autorité source de la nouvelle communauté[54]. L'autorité source de la nouvelle communauté peut être incorporée directement sous la "source" de l'ICP réceptrice et devenir ainsi un prestataire de services de certification subordonné au sein de cette ICP. Elle peut aussi devenir un prestataire de services de certification subordonné à l'un des prestataires de services de certification dans l'ICP existante. Une autre caractéristique attrayante des ICP hiérarchiques est qu'elles facilitent le développement de chemins de certification, parce qu'elles fonctionnent uniquement dans un sens, remontant du

[53] La question de savoir si un gouvernement devrait avoir la capacité technique de conserver ou de recréer des clefs de confidentialité privées peut être traitée au niveau de l'autorité source.

[54] William T. Polk et Nelson E. Hastings, *Bridge Certification Authorities: Connecting B2B Public Key Infrastructures*, National Institute of Standards and Technology (septembre 2000), accessible sur le site Internet: http://csrc.nist.gov/pki/documents/B2B-article.pdf (consulté le 5 juin 2008).

certificat de l'utilisateur au point de confiance. De plus, les chemins de certification au sein d'une ICP hiérarchique sont relativement courts, et les utilisateurs savent implicitement, à partir de la position occupée par le prestataire de services de certification, pour quelles applications un certificat peut être utilisé. Toutefois, les ICP hiérarchiques ont également des inconvénients, du fait surtout qu'elles s'appuient sur un seul point de confiance. Si l'autorité source est compromise, c'est toute l'ICP qui l'est. En outre, certains pays ont eu des difficultés à choisir une seule entité en tant qu'autorité source et à imposer cette hiérarchie à tous les autres prestataires de services de certification[55].

40. L'ICP dite "maillée" est une alternative à l'ICP hiérarchique. Dans ce modèle, les prestataires de services de certification sont liés par une relation de pair à pair. Tous peuvent être des points de confiance. En général, les utilisateurs feront confiance au prestataire de services de certification qui a émis leur certificat. Les prestataires de services de certification s'adressent mutuellement des certificats; la paire de certificats représente leur relation de confiance mutuelle. Du fait de l'absence de hiérarchie dans un tel système, les prestataires de services de certification ne peuvent imposer les conditions régissant les types de certificats émis par d'autres prestataires. Si un prestataire souhaite limiter la confiance accordée à d'autres prestataires, il doit préciser ces restrictions dans les certificats émis pour ses pairs[56]. Toutefois, il peut être très difficile d'harmoniser les conditions et les limites de la reconnaissance mutuelle.

41. Une troisième structure possible est l'architecture de prestataire de services de certification dite en "pont". Cette structure peut être particulièrement utile pour permettre à plusieurs communautés d'ICP existantes de se fier mutuellement à leurs certificats. Contrairement à un prestataire de services de certification dans une ICP maillée, un prestataire de services de certification pont n'émet pas directement de certificats aux utilisateurs. Il n'a pas non plus pour vocation de servir de point de confiance aux utilisateurs de l'ICP, comme c'est le cas d'une autorité source. En revanche, le prestataire de services de certification pont établit des relations de confiance de pair à pair avec les différentes communautés d'utilisateurs, ce qui permet à ces derniers de conserver leurs points de confiance naturels au sein de leur ICP respective. Si une communauté d'utilisateurs instaure un domaine de confiance sous la forme d'une ICP hiérarchique, le prestataire de services de certification pont établira une relation avec l'autorité source de cette ICP. Par contre, si elle instaure un domaine de confiance sous la forme d'une ICP maillée, le prestataire de services de certification pont devra uniquement établir une relation avec l'un des prestataires de services de certification de l'ICP, qui deviendra alors le principal prestataire de services de certification au sein de cette ICP en vue de l'établissement du "pont de confiance" avec l'autre ICP. Le pont de confiance qui relie deux ICP ou plus par le biais de leur relation mutuelle avec un prestataire de services de certification pont permet aux différentes communautés d'utilisateurs d'interagir les unes avec les autres pour un niveau de confiance donné grâce au prestataire de services de certification pont[57].

---

[55]Polk et Hastings (*Bridge Certification Authorities*…) observent qu'aux États-Unis, il a été très difficile de choisir une agence gouvernementale pour assumer un rôle d'autorité global sur l'ICP fédérale.

[56]Polk et Hastings, *Bridge Certification Authorities* ...

[57]Le prestataire de services de certification pont est la structure qui a finalement été retenue pour le système ICP du Gouvernement fédéral des États-Unis (Polk et Hastings, *Bridge Certification Authorities* ...). C'est également le modèle suivi pour développer le système ICP du Gouvernement japonais.

ii) *Prestataire de services de certification*

42. Pour associer une paire de clefs à un signataire éventuel, un prestataire de services de certification (ou autorité de certification) délivre un certificat, enregistrement électronique qui indique la clef publique ainsi que le nom du titulaire du certificat identifié comme "sujet" de ce certificat et qui peut confirmer que le signataire éventuel identifié dans le certificat détient la clef privée correspondante. La fonction essentielle d'un certificat est d'associer une clef publique à un signataire précis. Un "destinataire" du certificat souhaitant se fier à une signature numérique créée par le signataire indiqué dans le certificat peut utiliser la clef publique figurant dans le certificat pour vérifier que la signature numérique a bien été créée avec la clef privée correspondante. Si cette vérification est positive, le destinataire est dans une certaine mesure techniquement assuré que le signataire a créé la signature numérique et que la portion du message utilisé pour la fonction de hachage (et, par conséquent, le message de données correspondant) n'a pas été modifiée depuis qu'on y a apposé la signature numérique.

43. Afin d'assurer l'authenticité du certificat, pour ce qui est tant de son contenu que de sa source, le prestataire de services de certification y appose une signature numérique. Celle-ci peut être vérifiée au moyen de la clef publique de ce prestataire figurant sur un autre certificat délivré par un autre prestataire (qui peut, mais ne doit pas nécessairement, être une autorité hiérarchiquement supérieure), et cet autre certificat peut à son tour être authentifié par la clef publique figurant sur un autre certificat encore, et ainsi de suite, jusqu'à ce que la personne devant se fier à la signature numérique soit convaincue de son authenticité. Un autre moyen possible de vérifier une signature numérique consiste à enregistrer cette signature numérique sur un certificat délivré par le prestataire de services de certification (parfois appelé "certificat source")[58].

44. Dans chaque cas, le prestataire de services de certification délivrant le certificat peut apposer une signature numérique sur son propre certificat pendant la période de validité de l'autre certificat utilisé pour vérifier sa signature numérique. Selon la législation de certains États, on pourrait inspirer la confiance dans la signature numérique du prestataire de services de certification en publiant dans un journal officiel la clef publique de celui-ci ou certaines données se rapportant au certificat source (par exemple, une "empreinte digitale numérique").

45. Une signature numérique correspondant à un message, qu'elle soit créée par le signataire pour authentifier un message ou par un prestataire de services de certification pour authentifier son certificat, devrait généralement être horodatée de manière fiable pour permettre au vérificateur de déterminer si elle a bien été créée pendant la période de validité indiquée dans le certificat, et si le certificat était valable (par exemple, ne figurait pas sur une liste de révocation) au moment considéré, ce qui est l'une des conditions de la vérifiabilité d'une signature numérique.

46. Pour qu'une clef publique et son association à un signataire spécifique soient aisément vérifiables, le certificat peut être publié dans un répertoire ou mis à disposition par d'autres moyens. Généralement, les répertoires sont des bases de données en

[58] *Loi type de la CNUDCI sur les signatures électroniques*…, paragraphe 54 de la deuxième partie.

ligne regroupant des certificats et d'autres informations pouvant être appelés et utilisés pour vérifier les signatures numériques.

47. Une fois délivré, un certificat peut se révéler sujet à caution, par exemple si le signataire a donné une fausse identité au prestataire de services de certification. Dans d'autres cas, un certificat peut être fiable au moment où il est délivré, mais perdre sa fiabilité par la suite. Si la clef privée est compromise, par exemple parce que son signataire en a perdu le contrôle, le certificat peut perdre sa fiabilité et le prestataire de services de certification (à la demande du signataire ou même sans son consentement, selon les circonstances) peut alors suspendre (interrompre provisoirement la période de validité) ou révoquer (annuler définitivement) le certificat. On peut attendre du prestataire de services de certification que, peu après cette suspension ou cette révocation, il publie une notification de la révocation ou en avise les personnes qui l'interrogent ou dont il sait qu'elles ont reçu une signature numérique vérifiable par référence à un certificat qui n'est pas fiable. De même, le cas échéant, on devrait également examiner s'il y a eu révocation du certificat du prestataire de services de certification, ainsi que du certificat émis pour la vérification de la signature de l'autorité d'horodatage et du certificat du prestataire de services de certification qui a émis le certificat de l'autorité d'horodatage.

48. Les autorités de certification pourraient être des organismes relevant de l'État ou des prestataires de services privés. Dans quelques pays, on envisage, pour des raisons d'ordre public, que seuls des organismes publics soient autorisés à assurer la fonction de certification. Toutefois, dans la plupart des pays, soit les services de certification sont entièrement laissés au secteur privé, soit les organismes gérés par l'État coexistent avec des prestataires de services privés. Il y a aussi des systèmes de certification fermés, dans lesquels de petits groupes établissent leur propre prestataire de services de certification. Dans certains pays, les organismes relevant de l'État émettent des certificats uniquement à l'appui des signatures numériques utilisées par l'administration publique. Quelle que soit l'option retenue, et que les autorités de certification aient ou non besoin d'une licence pour fonctionner, une infrastructure à clef publique comprend généralement plusieurs prestataires de services de certification. Ce qui est particulièrement important est la relation entre les différentes autorités de certification (voir paragraphes 38 à 41 ci-dessus).

49. Il peut incomber au prestataire de services de certification ou à l'autorité source de veiller à ce que ses prescriptions soient systématiquement respectées. Si la sélection des autorités de certification peut se faire sur la base d'un certain nombre de facteurs, dont la solidité de la clef publique utilisée et l'identité de l'utilisateur, la fiabilité d'un prestataire de services de certification peut également dépendre de la façon dont il applique les normes de délivrance des certificats et de la fiabilité de son évaluation des données communiquées par les utilisateurs qui demandent ces certificats. Le régime de responsabilité qui s'applique à tout prestataire de services de certification est d'une importance cruciale eu égard à son respect des prescriptions en matière de politique générale et de sécurité édictées par l'autorité source ou par le prestataire de services de certification de niveau plus élevé, ou de toute autre prescription applicable, et ce de manière permanente. L'obligation du prestataire de services de certification d'agir en conformité avec les déclarations qu'il a faites en ce qui concerne ses politiques et pratiques, comme prévu à l'alinéa *a)* du paragraphe 1 de l'article 9 de la Loi type sur les signatures électroniques, est tout aussi importante.

c) Problèmes pratiques dans la mise en œuvre de l'infrastructure à clef publique

50. En dépit des connaissances considérables sur les technologies des signatures numériques et leur mode de fonctionnement, la mise en œuvre des systèmes d'infrastructure à clef publique et de signature numérique a, dans la pratique, connu quelques problèmes qui ont modéré l'utilisation des signatures numériques, restée de ce fait en deçà des attentes.

51. Les signatures numériques fonctionnent bien lorsqu'il s'agit de vérifier des signatures créées pendant la période de validité d'un certificat. Mais, une fois que le certificat a expiré ou été révoqué, la clef publique correspondante perd sa validité, même si la paire de clefs n'était pas compromise. Par conséquent, il faudrait qu'un système d'infrastructure à clef publique bénéficie d'une gestion des signatures numériques pour garantir la disponibilité de la signature dans le temps. La principale difficulté provient du risque que le document électronique "original" (c'est-à-dire les chiffres binaires – ou "bits" – qui constituent le fichier informatique dans lequel l'information est enregistrée), y compris la signature numérique, devienne illisible ou peu fiable avec le temps, en raison principalement de l'obsolescence du logiciel, du matériel ou des deux. De plus, la signature numérique peut devenir peu sûre en raison des progrès scientifiques en analyse cryptographique, le logiciel de vérification des signatures peut ne pas être disponible sur de longues périodes ou le document peut perdre son intégrité[59]. Il en résulte que la conservation à long terme des signatures électroniques est généralement problématique. Même si on a cru pendant un certain temps que les signatures numériques étaient indispensables à des fins d'archivage, l'expérience a montré qu'elles n'étaient pas à l'abri des risques à long terme. Comme toute altération du document après la création de la signature entraînera l'échec de la vérification de cette dernière, les opérations de reformatage destinées à préserver la lisibilité d'un document (comme la migration ou la conversion des données) peuvent affecter la durabilité de la signature[60]. En réalité, les signatures numériques ont été conçues davantage pour assurer la sécurité de la communication d'informations que pour préserver

[59] Jean-François Blanchette, "Defining electronic authenticity: an interdisciplinary journey", accessible sur le site Internet: http://polaris.gseis.ucla.edu/blanchette/papers/dsn.pdf (consulté le 5 juin 2008) (document publié dans un volume supplémentaire de la Conférence internationale sur la sûreté de fonctionnement des systèmes et des réseaux (DSN 2004), Florence (Italie), 28 juin-1er juillet 2004), pages 228 à 232.

[60] "En fin de compte, tout ce que nous pouvons préserver dans un contexte électronique sont les bits. Toutefois, nous savons depuis longtemps qu'il est très difficile de conserver une série de bits indéfiniment. Avec le temps, elle devient illisible (pour l'ordinateur et, partant, pour l'homme) en raison de l'obsolescence technologique du logiciel d'application et/ou du matériel (par exemple le lecteur). Jusqu'à présent, le problème de la durabilité des signatures numériques fondées sur une ICP a été mal étudié en raison de sa complexité. ... Bien que les outils d'authentification utilisés dans le passé, comme les signatures manuscrites, les sceaux, les tampons, les empreintes digitales, etc. soient également sujets au reformatage (par exemple le microfilm) en raison de l'obsolescence du support papier, ils ne deviennent jamais complètement inutilisables après une telle opération. Il y a toujours au moins une copie qui peut être comparée avec d'autres outils d'authentification d'origine". (Jos Dumortier et Sofie Van den Eynde, *Electronic Signatures and Trusted Archival Services*, page 5, accessible sur le site Internet: http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where= (consulté le 5 juin 2008).

les informations dans le temps[61]. Les initiatives visant à résoudre ce problème n'ont pas encore débouché sur une solution durable[62].

52. Un autre domaine dans lequel les systèmes de signature numérique et d'ICP peuvent poser des problèmes pratiques est celui de la sécurité des données et de la protection de la vie privée. Les prestataires de services de certification doivent garder en sécurité les clefs utilisées pour signer les certificats émis en faveur de leurs clients et risquent d'être exposés à des tentatives de tiers visant à obtenir un accès non autorisé à ces clefs (voir également les paragraphes 223 à 226 dans la deuxième partie). De plus, ils doivent obtenir une série de données personnelles et d'informations commerciales des personnes qui demandent un certificat. Les prestataires de services de

[61]En 1999, des archivistes de différents pays ont lancé le projet InterPARES (Recherche internationale sur les documents authentiques permanents dans les systèmes électroniques) pour "accroître les connaissances théoriques et méthodologiques essentielles à la conservation à long terme de documents authentiques créés et/ou conservés sous forme numérique" (voir http://www.interpares.org (consulté le 5 juin 2008)). Le projet de rapport du Groupe de travail sur l'authenticité, accessible sur le site Internet: http://www.interpares.org/documents/atf_draft_final_report.pdf (consulté le 5 juin 2008), qui faisait partie de la première phase du projet (InterPARES 1, achevée en 2001) concluait que "les signatures numériques et les infrastructures à clef publique (ICP) sont des exemples de technologies développées et mises en œuvre pour authentifier des documents électroniques transmis d'un endroit à un autre. Même si les archivistes et les informaticiens ont confiance dans les technologies d'authentification pour garantir l'authenticité des documents, ces technologies n'ont jamais été destinées, et n'en ont pas l'aptitude à l'heure actuelle, à assurer l'authenticité de documents électroniques dans la durée". Le rapport final d'InterPARES 1 est accessible sur le site Internet: http://www.interpares.org/book/index.htm. La suite du projet (InterPARES 2) a pour objectif de développer et d'élaborer des concepts, des principes, des critères et des méthodes pour la création et la préservation de documents exacts et fiables et la conservation à long terme de documents authentiques dans le contexte des activités artistiques, scientifiques et gouvernementales menées entre 1999 et 2001.

[62]L'Initiative européenne de normalisation des signatures électroniques (EESSI), par exemple, a été créée en 1999 par le Conseil de normalisation des TIC, groupe d'organisations s'occupant conjointement de la normalisation et des activités connexes dans les technologies de l'information et de la communication, établi afin de coordonner les activités de normalisation à l'appui de la mise en œuvre de la directive de l'Union européenne sur les signatures électroniques (voir *Journal officiel des communautés européennes*, L 13/12, 19 janvier). Le consortium EESSI (initiative de normalisation qui s'emploie à traduire les exigences de la directive européenne sur les signatures électroniques en normes européennes) cherchait à répondre au besoin de la conservation à long terme de documents à signature cryptographique au moyen de sa norme sur les formats de signature électronique (normes Electronic Signature Format ES 201 733, ETSI, 2000). Le format distingue des moments dans la validation de la signature, la validation initiale et une validation ultérieure. Le format de cette dernière réunit toutes les informations qui peuvent être utilisées dans le processus de validation, comme les informations relatives à la révocation, l'horodatage, les politiques de signature, etc. Ces informations sont réunies lors de l'étape de la validation initiale. Les concepteurs de ce format de signature électronique étaient préoccupés par la menace que faisait peser le déclin de la force cryptographique sur la validité de la signature. Pour lutter contre cette menace, les signatures EESSI sont régulièrement horodatées à nouveau, avec des algorithmes de signature et des tailles de clef adaptées aux méthodes d'analyse cryptographique les plus récentes. Le problème de la longévité des logiciels a été traité dans un rapport de l'EESSI datant de 2000, qui introduisait les "opérateurs fiables de services d'archivage", nouveau type de service commercial qui serait proposé par des professions et des organes compétents qui restent à définir, afin de garantir la conservation à long terme de documents à signature cryptographique. Le rapport énumère un certain nombre d'exigences techniques auxquelles ces opérateurs devraient satisfaire, dont la "compatibilité rétroactive" avec les logiciels et le matériel informatiques, par la conservation de l'équipement ou par l'émulation (voir Blanchette, "Defining electronic authenticity ...". Une étude complémentaire sur la recommandation de l'EESSI relative aux opérateurs fiables de services d'archivage réalisée par le Centre interdisciplinaire pour le droit et les technologies de l'information de la Katholieke Universiteit Leuven, Belgique, intitulée *European Electronic Signature Standardization Initiative: Trusted Archival Services* (phase 3, rapport final, 28 août 2000), peut être consultée à l'adresse Internet: http://www.law.kuleuven.ac.be/icri/publications/91TAS-Report.pdf?where= (consulté le 5 juin 2008). L'EESSI a cessé ses activités en octobre 2004. Les systèmes permettant d'appliquer les recommandations de l'EESSI ne semblent pas être opérationnels à l'heure actuelle (voir Dumortier et Van den Eynde, *Electronic Signatures and Trusted Archival Services…*).

certification doivent conserver ces informations en vue d'une utilisation ultérieure. Ils doivent prendre les mesures nécessaires pour que l'accès à ces informations soit conforme aux lois applicables en matière de protection des données[63]. Malgré tout, la menace d'un accès non autorisé reste bien réelle.

2. Biométrie

53. Un identificateur biométrique est une mesure servant à identifier une personne par ses caractéristiques physiques ou comportementales. Les caractéristiques susceptibles d'être utilisées pour la reconnaissance biométrique sont l'ADN; les empreintes digitales; l'iris; la rétine; la forme de la main ou du visage; la thermographie faciale; la forme de l'oreille; la voix; l'odeur corporelle; le dessin des vaisseaux sanguins; l'écriture; la démarche et la dynamique de frappe.

54. Le recours à des dispositifs biométriques implique en général de prélever, sous forme numérique, un échantillon biométrique d'une caractéristique biologique d'une personne. Les données biométriques sont ensuite extraites de l'échantillon pour créer un modèle de référence. L'identité de la personne à laquelle correspond l'échantillon biométrique est confirmée, ou l'authenticité des communications provenant prétendument de cette personne est vérifiée par comparaison des données biométriques avec celles stockées dans le modèle de référence[64].

55. Les techniques biométriques mettent en jeu des risques liés à la conservation des données biométriques car, en général, les caractéristiques biométriques ne peuvent être contestées. Lorsque des systèmes biométriques ont été compromis, l'utilisateur légitime n'a pas d'autre choix que d'abandonner les données d'identification et d'adopter un autre ensemble, non compromis. Des règles spéciales sont donc nécessaires pour empêcher l'utilisation abusive des bases de données biométriques.

56. L'exactitude des techniques biométriques ne peut être absolue, car les caractéristiques biologiques tendent par essence à être variables, et toute mesure peut comporter un écart. À cet égard, les données biométriques ne sont pas considérées comme des identificateurs uniques, mais plutôt semi-uniques. Pour tenir compte de ces variations,

---

[63] Voir les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (Paris, 1980), accessible sur le site Internet: http://www.oecd.org/document/0,2340,fr_2649_34255_1815225_1_1_1_1,00.html (consulté le 5 juin 2008); la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Conseil de l'Europe, *Série des traités européens* n° 108), accessible sur le site Internet: http://conventions.coe.int/treaty/FR/Treaties/Html/108.htm, consulté en juin 2008; les Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel (résolution 45/95 de l'Assemblée générale); et la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (*Journal officiel des communautés européennes*, L 281, 23 novembre 1995, accessible sur le site Internet: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (consulté en juin 2008).

[64] International Association for Biometrics et International Computer Security Association (copie disponible au secrétariat).

on peut jouer sur l'exactitude des données en fixant le seuil de correspondance entre le modèle de référence et l'échantillon prélevé. Toutefois, un seuil bas risque d'introduire une distorsion dans le sens de fausses acceptations, et un seuil élevé est susceptible de favoriser les faux rejets. Cela dit, l'exactitude de l'authentification fournie par la biométrie peut être suffisante dans la majorité des applications commerciales.

57. De plus, la conservation et la divulgation des données biométriques suscitent des questions concernant la protection des données et les droits de l'homme. Bien qu'elles ne se réfèrent peut-être pas expressément à la biométrie, les lois sur la protection des données[65] ont pour objectif de protéger les données des personnes physiques et le traitement de ces données, qu'il s'agisse des données brutes ou de modèles, sont au cœur de la technologie biométrique[66]. De plus, des mesures peuvent être requises pour protéger les consommateurs contre les risques découlant de l'utilisation privée des données biométriques, ainsi qu'en cas de vol d'identité. D'autres domaines juridiques, notamment le droit du travail et de la santé, peuvent également entrer en ligne de compte[67].

58. Des solutions techniques pourraient aider à répondre à certaines préoccupations. Par exemple, la conservation de données biométriques sur des cartes à puce ou des jetons peut prévenir un accès non autorisé, qui pourrait se produire si les données sont stockées dans un système d'information centralisé. De plus, des pratiques optimales ont été mises au point pour réduire les risques dans différents domaines tels que le champ d'application et les capacités, la protection des données, le contrôle de l'utilisation des données personnelles, et la divulgation, la vérification, la responsabilité et la surveillance[68].

59. On considère généralement que les dispositifs biométriques offrent un niveau élevé de sécurité. Bien qu'ils soient compatibles avec de nombreuses applications, ils sont surtout utilisés actuellement par les gouvernements, en particulier dans le domaine de la sécurité, notamment pour les vérifications en matière d'immigration et pour les contrôles d'accès.

60. Des applications commerciales ont aussi vu le jour, qui utilisent souvent la biométrie dans des authentifications à double facteur exigeant la fourniture d'un élément propre à la personne (identificateur biométrique) et d'un élément dont cette dernière a connaissance (généralement un mot de passe ou PIN). En outre, des applications ont

---

[65]Voir note 63.

[66]Paul de Hert, *Biométrie: questions et incidences juridiques*, document d'information pour l'Institute for Prospective Technological Studies de la Commission européenne (Communautés européennes, Direction générale du Centre commun de recherche, 2005), page 13, accessible sur le site Internet: http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf. (consulté le 5 juin 2008).

[67]Au Canada, par exemple, l'utilisation de la biométrie a été examinée par rapport à la mise en œuvre de la Loi sur la protection des renseignements personnels et les documents électroniques (2000, ch. 5) sur le lieu de travail (voir *Turner c. TELUS Communications Inc.*, 2005 CF 1601, 29 novembre 2005 (Cour fédérale du Canada)).

[68]À titre d'illustration de ces pratiques optimales, voir l'initiative de l'International Biometric Group sur la biométrie et la vie privée, "Best practices for privacy-sympathetic biometric deployment", accessible sur le site Internet: http://www.bioprivacy.org (consulté le 5 juin 2008).

été mises au point pour enregistrer et comparer les caractéristiques d'une signature manuscrite. Des tablettes graphiques basées sur la technologie numérique enregistrent la pression du stylet et la durée du processus de signature. Ces données sont ensuite conservées sous la forme d'un algorithme utilisé pour comparer les signatures futures. Toutefois, en raison des caractéristiques inhérentes à la biométrie, la prudence est de mise face aux dangers d'un renforcement progressif et non contrôlé de son utilisation dans les opérations commerciales courantes.

61. Le remplacement des signatures manuscrites par des signatures biométriques risque de poser un problème de preuve. Comme il a été indiqué plus haut, la fiabilité des preuves biométriques varie en fonction des technologies utilisées et du taux de fausses acceptations choisi. De plus, il est possible de manipuler ou de falsifier les données biométriques enregistrées sous forme numérique.

62. Les critères généraux de fiabilité prévus dans la Loi type de la CNUDCI sur les signatures électroniques et celle, plus récente, sur le commerce électronique, peuvent s'appliquer à l'utilisation des signatures biométriques. Dans un souci d'uniformité, il pourrait également être utile d'élaborer des lignes directrices internationales relatives à l'utilisation et à la gestion des méthodes biométriques, plus récentes[69]. Dans un souci d'uniformité, il pourrait également être utile d'élaborer des lignes directrices internationales relatives à l'utilisation et à la gestion des méthodes biométriques[70]. Il faut toutefois examiner avec soin si de telles normes seraient ou non prématurées, compte tenu de l'état d'avancement actuel des technologies biométriques, et si elles risqueraient ou non d'en compromettre le développement permanent.

3. Mots de passe et méthodes hybrides

63. Mots de passe et codes sont utilisés à la fois pour contrôler l'accès à des informations ou à des services et pour "signer" des communications électroniques. Dans la pratique, cette deuxième utilisation est moins fréquente que la première, en raison du risque de compromettre le code s'il est transmis dans un message non codé. Toutefois, les mots de passe et les codes sont la méthode d'"authentification" la plus utilisée pour les contrôles d'accès et la vérification de l'identité, dans de nombreuses opérations, y compris pour la plupart des opérations bancaires en ligne, les retraits d'espèces aux guichets automatiques et les transactions par carte de crédit.

64. Il faut observer que de multiples technologies peuvent être utilisées pour "authentifier" une transaction électronique. On peut recourir à plusieurs technologies ou à plusieurs utilisations d'une même technologie pour une seule transaction. Par

[69]Le projet de Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux a été approuvé par la CNUDCI à sa trente-huitième session (Vienne, 4-15 juillet 2005). La Convention a été adoptée par l'Assemblée générale, dans sa résolution 60/21 du 23 novembre 2005.

[70]On pourra comparer avec les critères de fiabilité présentés dans le Guide pour l'incorporation de la Loi type de la CNUDCI sur les signatures électroniques (*Loi type de la CNUDCI sur les signatures électroniques* …, paragraphe 75 de la deuxième partie.

exemple, la dynamique de la signature à des fins d'authentification peut être combinée avec la cryptographie pour garantir l'intégrité du message. Une autre possibilité consiste à communiquer des mots de passe sur Internet au moyen de la cryptographie (par exemple SSL dans les navigateurs) pour les protéger, et à utiliser en même temps la biométrie pour déclencher une signature numérique (cryptographie asymétrique) qui, à réception, génère un ticket Kerberos (cryptographie symétrique). L'élaboration de cadres généraux et juridiques pour traiter ces technologies devrait tenir compte du rôle des technologies multiples. Pour ce qui est de l'authentification électronique, de tels cadres devront être assez souples pour couvrir les solutions fondées sur des technologies hybrides, car des cadres axés sur des technologies spécifiques pourraient entraver l'utilisation de technologies multiples[71]. Des dispositions technologiquement neutres faciliteraient l'acceptation de telles solutions hybrides.

4. Signatures scannées et noms saisis au clavier

65. Le droit privé s'est surtout intéressé au commerce électronique en raison de la manière dont les nouvelles technologies pourraient influencer l'application de règles de droit conçues pour d'autres moyens de communication. Cet intérêt pour la technologie a souvent conduit, délibérément ou non, à mettre l'accent sur des technologies perfectionnées offrant un niveau élevé de sécurité pour les méthodes d'authentification et de signature électroniques. Dans ce contexte, on oublie souvent qu'une grande partie, sinon la majorité, des communications commerciales échangées dans le monde ne font appel à aucune technologie particulière d'authentification ou de signature.

66. Dans la pratique quotidienne, les entreprises du monde entier se contentent souvent, par exemple, d'échanges de courriers électroniques sans autre forme d'authentification ou de signature que le nom saisi au clavier, le titre et l'adresse des parties figurant à la fin du message. Parfois, elles recourent à une présentation plus formelle au moyen de fac-similés ou d'images scannées de signatures manuscrites qui, cela va de soi, ne sont qu'une copie numérisée d'un original manuscrit. Ni des noms saisis dans un courrier électronique non chiffré ni des signatures scannées n'offrent un niveau élevé de sécurité ou ne peuvent prouver avec certitude l'identité de l'auteur des communications électroniques dans lesquelles ils apparaissent. Néanmoins, les entités commerciales choisissent librement d'utiliser ces formes d'"authentification" pour des raisons de facilité, de rapidité et d'économie des communications. Il est important que les législateurs et les responsables politiques aient à l'esprit ces pratiques commerciales répandues lorsqu'ils envisagent de réglementer les méthodes d'authentification et de signature électroniques. Des exigences strictes en la matière, notamment l'imposition d'une méthode ou d'une technologie particulière pourraient, sans le vouloir, jeter des doutes sur la validité et la force exécutoire d'un nombre important de transactions réalisées tous les jours sans l'utilisation d'une méthode particulière d'authentification

[71] Voir le document *Signature Directive Consultation Compilation*, 28 octobre 1998, de la Foundation for Information Policy Research, qui propose une compilation des réponses apportées au cours des consultations sur le projet de directive de l'Union européenne sur les signatures électroniques, établie à la demande de la Commission européenne. Il est accessible sur le site Internet: www.fipr.org/publications/sigdirecon.html (consulté le 5 juin 2008).

ou de signature. Cela risque, par conséquent, d'inciter les parties de mauvaise foi à éviter les conséquences d'obligations qu'elles ont librement contractées en remettant en cause l'authenticité de leurs propres communications électroniques. Il n'est pas réaliste de penser que l'imposition d'un niveau élevé d'exigences en matière d'authentification et de signature, conduirait à terme toutes les parties à les utiliser au quotidien. Des expériences menées récemment avec des méthodes sophistiquées, telles que les signatures numériques, ont montré que les préoccupations de coût et de complexité mettaient souvent un frein à l'utilisation, dans la pratique, de techniques d'authentification et de signature.

C. Gestion de l'identité électronique

67. À l'ère de l'électronique, les personnes physiques ou morales peuvent accéder aux services d'un certain nombre de fournisseurs. Chaque fois qu'une personne s'inscrit auprès de l'un d'entre eux pour avoir accès à ses services, une "identité" électronique est créée. Par ailleurs, une identité unique peut être reliée à un certain nombre de comptes pour chaque application ou plate-forme. La multiplication des identités et de leurs comptes peut en compliquer la gestion, pour l'utilisateur comme pour le prestataire de services. Ces difficultés pourraient être évitées si chaque personne avait une seule identité électronique.

68. L'inscription d'une personne auprès d'un prestataire de services et la création d'une identité électronique entraînent l'établissement d'une relation de confiance mutuelle entre cette personne et le prestataire. La création d'une identité électronique unique suppose que l'on regroupe toutes ces relations bilatérales dans un cadre plus large où elles pourraient être gérées globalement, dans ce que l'on appelle un système de gestion de l'identité. Les avantages de la gestion de l'identité peuvent être, pour le fournisseur, une sécurité accrue, une plus grande facilité de respecter les règlements et une plus grande souplesse commerciale et, pour l'utilisateur, un accès facilité à l'information.

69. La gestion de l'identité peut donner lieu aux deux approches suivantes:

a) L'approche traditionnelle de l'accès utilisateur. Cette approche suit le paradigme de l'accès utilisateur (connexion), qui repose sur l'utilisation des informations contenues dans un dispositif tel qu'une carte à puce ou bien conservées de toute autre manière par le client, et que ce dernier utilise pour se connecter à un service. En matière de gestion de l'identité, l'approche accès utilisateur se concentre sur l'administration de l'authentification de l'utilisateur, les droits et restrictions d'accès, les profils des comptes, les mots de passe et autres attributs dans un ou plusieurs systèmes ou applications. Elle vise à faciliter et contrôler l'accès aux applications et aux ressources tout en protégeant les données personnelles et commerciales confidentielles vis-à-vis d'utilisateurs non autorisés;

b) L'approche des services. Il y a là un paradigme plus novateur, qui repose sur un système fournissant des services personnalisés aux utilisateurs et à leurs dispositifs. Avec cette approche, la gestion de l'identité a une portée plus vaste et comprend toutes les ressources de l'entreprise servant à fournir des services en ligne, comme l'équipement réseau, les serveurs, les portails, le contenu, les applications et les produits, de même que les certificats (credentials) de l'utilisateur, ses carnets d'adresses, ses préférences et ses droits. Dans la pratique, elle pourrait inclure, par exemple, des informations sur les paramètres du contrôle parental et la participation à des programmes de fidélité.

70. On s'emploie actuellement à développer la gestion de l'identité à la fois dans le monde des affaires et au niveau gouvernemental. Il faut toutefois noter que les grands choix, dans les deux scénarios, peuvent différer considérablement. L'approche gouvernementale, par exemple, visera peut-être plutôt à mieux répondre aux besoins des citoyens et penchera davantage vers l'interaction avec des personnes physiques. Pour leur part, les applications commerciales doivent tenir compte de l'utilisation croissante de machines automatisées dans les transactions commerciales et choisiront peut-être des caractéristiques destinées à répondre aux besoins spécifiques de ces machines.

71. Parmi les difficultés liées aux systèmes de gestion de l'identité figurent les questions de confidentialité, en raison des risques associés à l'utilisation abusive d'identificateurs uniques. En outre, des questions peuvent également se poser du fait des différences entre les règlements juridiques applicables, notamment en ce qui concerne la possibilité de déléguer le pouvoir d'agir pour le compte d'autrui. On a suggéré des solutions bâties autour d'une coopération commerciale volontaire fondée sur ce que l'on appelle le cercle de confiance, où les participants doivent se fier à l'exactitude et à la précision des informations qui leur sont fournies par d'autres membres du cercle. Cette approche ne suffira toutefois peut-être pas pour réglementer toutes les questions connexes et l'adoption d'un cadre juridique pourra rester nécessaire. Des lignes directrices ont également été élaborées pour offrir un cadre légal aux cercles d'infrastructures de confiance[72].

72. S'agissant de l'interopérabilité technique, l'Union internationale des télécommunications a établi un groupe spécialisé sur la gestion de l'identité afin de faciliter et promouvoir l'établissement d'un cadre générique pour la gestion de l'identité et les moyens d'identifier des identités distribuées de façon autonome ainsi que des fédérations d'identités[73].

73. Des solutions de gestion de l'identité sont également apportées dans le cadre de l'administration en ligne. Ainsi, dans le contexte de la stratégie de l'Union européenne:

[72]Le Liberty Alliance Project (voir: www.projectliberty.org) est une alliance mondiale qui regroupe plus de 150 entreprises, organisations à but non lucratif et agences gouvernementales. Le consortium tente de développer une norme ouverte d'identité de réseaux fédérée prenant en charge tous les périphériques de réseaux actuels et futurs. L'identité fédérée offre aux entreprises, aux gouvernements, aux employés et aux consommateurs un moyen plus pratique et plus sécurisé de contrôler les paramètres d'identité dans l'économie numérique d'aujourd'hui, ce qui en fait un élément essentiel dans la mise en œuvre du cybercommerce, de services de données personnalisés et de services Internet. L'adhésion est ouverte à toutes les organisations commerciales et non commerciales.

[73]Voir: http://www.itu.int/ITU-T/studygroups/com17/fgidm/index.html (consulté le 20 mars 2008).

"i2010: une société de l'information pour la croissance et l'emploi"[74], une étude sur la gestion de l'identité dans l'administration en ligne a été lancée pour encourager les progrès tendant à une approche cohérente en la matière dans l'Union européenne, sur la base des connaissances et des initiatives existantes dans les États membres de l'Union européenne[75].

74. Les dispositifs de signature électronique, qui prennent souvent la forme de cartes à puce, sont des initiatives de plus en plus fréquentes parmi celles prises pour les besoins des administrations gouvernementales en ligne. Des opérations de distribution de cartes à puce ont été lancées à l'échelle nationale, entre autres, en Belgique, où elles ont été introduites initialement dans un certain nombre de provinces en 2003[76], pour être finalement étendues à tout le pays, à la suite d'une période d'essai concluante[77]. Le système belge consiste essentiellement en l'émission de cartes d'identité matérielles équipées d'une puce qui contient les données dont le citoyen a besoin pour produire une signature numérique[78].

75. L'Autriche a élaboré un système de gestion de l'identité qui enregistre des attributs d'identification pour chaque citoyen autrichien, mais qui n'intègre pas ces attributs dans les documents officiels d'identification de celui-ci. Au lieu de cela, l'Autriche a choisi des normes technologiquement neutres et, en conséquence, une gamme de solutions technologiques ont été élaborées et adoptées par les consommateurs. Le système autrichien s'appuie sur un "lien entre la personne et l'identité", c'est-à-dire une structure signée par l'autorité publique émettrice qui assigne un trait d'identification unique d'une personne (par exemple un numéro d'enregistrement) à un ou plusieurs certificats appartenant à cette personne. En tant que tel, le lien de la personne peut être utilisé pour l'identification unique et automatisée d'une personne quand celle-ci approche l'autorité publique lors d'une procédure[79]. Chaque particulier pourra choisir de conserver ce "trait d'identification unique" dans toute carte à puce de son choix (par exemple une carte (de débit) ATM (guichet automatique), carte de sécurité sociale, carte d'identité d'étudiant, carte de membre d'un syndicat ou d'une association professionnelle, ordinateur PC ou portable). Les dispositifs de signature peuvent aussi

---

[74]Communication de la Commission des communautés européennes au Conseil européen, au Parlement européen, au Comité économique et social et au Comité des régions: "i2010 – Une société de l'information pour la croissance et l'emploi", COM(2005) 229 final, (Bruxelles, 1er juin 2005), accessible sur le site Internet: http://eur-lex.europa.eu (consulté le 20 mars 2008).

[75]Voir *Modinis Study on Identity Management in eGovernment: Identity Management Issue Report* (Commission européenne, Direction générale, Société de l'information et médias, 18 septembre 2006), pages 9 à 12, accessible sur le site Internet: https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi (consulté le 6 juin 2008).

[76]La carte d'identité électronique a été introduite en Belgique en 2003 par la Loi du 25 mars 2003 modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant le loi du 8 août 1983 organisant un Registre national des personnes physiques (*Moniteur belge,* éd. 4, 28 mars 2003, page 15921).

[77]Voir l'Arrêté royal du 1er septembre 2004 portant la décision de procéder à l'introduction généralisée de la carte d'identité électronique (*Moniteur belge,* éd. 2, 15 septembre 2004, page 56527). Pour des informations générales, voir: http://eid.belgium.be (consulté le 6 juin 2008).

[78]Pour des informations générales voir: http://eid.belgium.be (consulté le 6 juin 2008).

[79]Zentrum für sichere Informationstechnologie Austria (A-Sit), *XML Definition of the Person Identity Link* (accessible sur le site Internet: http://www.buergerkarte.at/konzept/personenbindung/spezifikation/aktuell (consulté le 6 juin 2008).

être transmis par téléphone mobile sous la forme de codes à usage unique générés spécifiquement par le prestataire de service de téléphonie mobile, qui fait fonction de dépositaire du trait d'identification unique du citoyen.

76. Ce système permet d'émettre des identifiants spécifiques de secteur qui demeurent strictement cloisonnés, mais qui sont reliés à un système de stockage central des identités. Cette architecture exclue les questions de partage des données et assure la protection des données relatives à la vie privée. Les "cartes de citoyens" ambitionnent de devenir les documents d'identité officiels pour les procédures administratives électroniques, telles que les dépôts de candidatures par l'Internet. La carte de citoyen met une infrastructure sécurisée à la disposition de tous, notamment les clients des entreprises commerciales. Des sociétés peuvent élaborer des services en ligne sécurisés pour leurs clients à partir de l'infrastructure offerte par la carte de citoyen.

77. En conséquence des initiatives telles que celles décrites ci-dessus, un très grand nombre de citoyens sont en possession des dispositifs permettant notamment de sécuriser des signatures électroniques, à un coût faible. Bien que l'objectif premier de ces initiatives ne soit peut-être pas commercial, de tels dispositifs peuvent également être utilisés dans un environnement commercial. On reconnaît de plus en plus la convergence de ces deux domaines d'application[80].

[80]Voir, par exemple, le *Livre blanc coréen sur Internet* (Séoul, Agence nationale coréenne de développement d'Internet, 2006), page 81, qui se réfère à la double utilisation, dans le gouvernement en ligne et dans le commerce électronique, de la loi sur les signatures électroniques, de la République de Corée, accessible sur le site Internet: http://www.ecommerce.or.kr/activities/documents_view.asp?bNo=642&Page=1 (consulté le 6 juin 2008).

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

78. Le commerce électronique ne peut se développer que dans un climat de confiance. Des règles spéciales peuvent être nécessaires pour que son utilisation soit plus certaine et plus sûre. Ces règles peuvent revêtir la forme de textes législatifs très divers: instruments juridiques internationaux (traités et conventions), lois-types transnationales, législations nationales (fréquemment fondées sur les lois types), instruments d'autorégulation[81]; ou accords contractuels[82].

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

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

[81]Voir, par exemple, Commission économique pour l'Europe, Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques, recommandation nº 32 – "Instruments d'autorégulation du commerce électronique (codes de conduite)", (ECE/TRADE/277) accessible sur le site Internet: http://www.unece.org/cefact/recommendations/rec_index.htm (consulté le 5 juin 2008).

[82]Beaucoup d'initiatives, aux échelons national et international, visent à élaborer des contrats-types, (voir, par exemple, Commission économique pour l'Europe, Groupe de travail sur la facilitation des procédures du commerce international, recommandation n° 26 – "Utilisation commerciale d'accords d'échange aux fins de l'échange de données informatisé" (TRADE/WP.4/R.1133/Rec.1), et recommandation n° 31 – "Accords de commerce électronique" (ECE/TRADE/257), accessibles sur le site Internet: http://www.unece.org/cefact/recommendations/rec_index.htm (consulté le 5 juin 2008).

diverses comme "règles du système", "règles de fonctionnement" ou "accords entre partenaires commerciaux", conçus de manière à fournir et garantir la fonctionnalité, la fiabilité et la sécurité opérationnelles nécessaires aux membres du groupe. Ces règles et accords traitent fréquemment de question comme la reconnaissance de la valeur juridique des communications électroniques, la date et le lieu d'expédition et de réception des messages de données, les procédures de sécurité à suivre pour avoir accès au réseau ou les méthodes d'authentification ou de signature devant être employées par les parties[83]. Dans les limites de la liberté contractuelle reconnues par le droit applicable, ces règles et accords sont habituellement d'application directe.

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

A. Approche technologique des textes législatifs

82. Les lois et règlements relatifs aux méthodes d'authentification électroniques élaborés aux plans national et international ont revêtu de nombreuses formes différentes. On peut distinguer essentiellement trois approches des méthodes d'authentification et de signature: *a)* l'*approche minimaliste*; *b)* l'*approche technospécifique;* et *c)* l'*approche dualiste*[84]**.**

1. Approche minimaliste

83. Quelques pays qui suivent une politique de neutralité technologique reconnaissent de ce fait toutes les méthodes de signature électronique[85]. Cette approche est également appelée minimaliste car elle ne confère qu'un statut juridique minimum aux différentes formes de signature électronique. Selon cette approche minimaliste, les signatures électroniques sont considérées comme l'équivalent fonctionnel de signatures manuscrites à condition que la technologie employée soit conçue de manière à aboutir à certains résultats spécifiés et, par ailleurs, réponde à certaines exigences de fiabilité.

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

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

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

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

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

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

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

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

86. Beaucoup de pays ont intégré ce principe général dans leur législation. Le principe de neutralité technologique permet également d'accueillir l'évolution future de la technologie. En outre, cette approche privilégie la liberté des parties de choisir la technologie la mieux adaptée à leurs besoins. Il appartient alors aux parties de déterminer le degré de sécurité qu'elles jugent suffisant pour leurs communications. Cela permet d'éviter une complexité technologique excessive et les surcoûts correspondants[86].

87. Sauf en Europe, où la législation a été surtout influencée par les directives de l'Union européenne[87], la plupart des pays qui ont promulgué des textes concernant le commerce électronique ont utilisé la Loi type sur le commerce électronique comme un

[86]Mason, "Electronic signatures in practice", *Journal of High Technology Law,* vol. VI, nº.2 (2006), page153.

[87]En particulier, la directive CE/1999/93 du Parlement européen et du Conseil relative à l'établissement d'un cadre communautaire pour les signatures électroniques, (*Journal officiel des Communautés européennes*, L 13, 19 janvier 2000). La directive sur les signatures électroniques a été suivie d'un texte plus général, la directive CE/2000/31 du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, en particulier le commerce électronique, sur le marché interne (*Journal officiel des Communautés européennes*, nº. L 178, 17 juillet 2000), qui a trait à divers aspects de la fourniture de services informatiques et des contrats électroniques.

modèle[88]. La Loi type a également servi de base à l'harmonisation, au plan national, des lois relatives au commerce électronique d'États fédéraux comme le Canada[89] et les États-Unis[90]. À de rares exceptions près[91], les pays qui ont promulgué des textes d'application de la Loi type ont préservé son approche technologiquement neutre et n'ont ni prescrit, ni privilégié l'utilisation d'une méthode spécifique. Aussi bien la Loi type de la CNUDCI sur les signatures électroniques (adoptée en 2001), que la plus récente Convention des Nations Unies sur l'utilisation des communications électroniques dans les

[88]En janvier 2007, les pays suivants (liste éventuellement non exhaustive) avaient adopté des lois incorporant des dispositions de la Loi type de la CNUDCI sur le commerce électronique: Afrique du sud, *Electronic Communications and Transactions Act (2002)*; Australie, *Electronic Transactions Act 1999*; Chine, Loi de 2004 relative aux signatures électroniques; Colombie, *Ley de comercio electrónico*; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos (2002)*; France, *Loi 2000-230 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (2000);* Inde, *Information Technology Act, 2000*; Irlande, *Electronic Commerce Act, 2000*; Jordanie, *Electronic Transactions Law, 2001*; Maurice, *Electronic Transactions Act, 2000*; Mexique, *Decreto por el que se reforman y adicionan diversas disposiciones del código civil para el Distrito Federal en materia federal, del Código federal de procedimientos civiles, del Código de comercio y de la Ley federal de protección al consumidor (2000)*; Nouvelle-Zélande, *Electronic Transactions Act, 2002*; Pakistan, *Electronic Transactions Ordinance, 2002*; Panama, *Ley de firma digital (2001)*; Philippines, *Electronic Commerce Act (2000)*; République de Corée, *Loi-cadre de 2001 relative au commerce électronique;* République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*; Singapour, *Electronic Transactions Act (1998)*; Slovénie, *Loi de 2000 relative au commerce et aux signatures électroniques;* Sri Lanka, *Electronic transactions Act (1998)*; Thaïlande, *Electronic transactions Act (2001)*; Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas (2001)*; et Viet Nam, Loi de 2006 relative aux transactions électroniques. La Loi type a également été adoptée dans les baillages dépendant de la Couronne britannique de Guernesey *(Electronic Transactions (Guernsey) Law 2000),* et de Jersey (*Electronic Communications (Jersey) Law 2000*) ainsi que dans l'île de Man *(Electronic Transactions Act 2000)*; dans les territoire britanniques d'outre-mer des Bermudes *(Electronic Transactions Act 1999)*, îles Caïman (*Electronic Transactions Act 2000*) et îles Turques et Caïques (*Electronic Transactions Ordinance 2000*); et la Région administrative spéciale chinoise de Hong Kong (SAR) (*Electronic Transactions Ordinance (2000)*). Sauf indication contraire, les références qui sont faites ci-après à la législation des pays indiqués se rapportent aux dispositions des textes énumérés ci-dessus.

[89]Au Canada, le texte d'application de la Loi type est la *Loi uniforme relative au commerce électronique*, adoptée en 1999 par la Conférence pour l'harmonisation des lois au Canada (accessible, avec un commentaire officiel, à l'adresse: http://www.chlc.ca/en/poam2/index.cfm?sec=1999&sub=1999ia (consulté le 6 juin 2008). Cette loi a depuis lors été promulguée par plusieurs provinces et territoires, dont l'Alberta, la Colombie britannique, l'île du Prince Edward, le Labrador, le Manitoba, le Nouveau Brunswick, la Nouvelle-Écosse, l'Ontario, le Saskatchewan, Terre-Neuve et le Yukon. La Province du Québec a adopté une loi spécifique (Loi concernant le cadre juridique des technologies de l'information, 2001) qui, bien que de portée plus générale et rédigée très différemment, répond à bien des égards aux mêmes objectifs que la Loi uniforme relative au commerce électronique et est généralement conforme à la Loi type de la CNUDCI. On trouvera les dernières informations disponibles concernant la promulgation de la Loi uniforme à l'adresse http://www.chlc.ca/en/cls/index.cfm?sec=4&sub=4b> (consulté le 5 juin 2008).

[90]Aux États-Unis, la Conférence nationale des commissaires sur la loi uniforme (Conférence of Commissioners on Uniform State Law) s'est fondée sur la Loi type de la CNUDCI sur le commerce électronique pour élaborer la loi uniforme sur les transactions électroniques, adoptée en 1999 (le texte de cette loi, et son commentaire officiel, est accessible sur le site Internet: http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm (consulté le 6 juin 2008). La loi a, depuis lors, été promulguée dans le District de Columbia et les 46 États suivants: Alabama, Alaska, Arizona, Arkansas, Californie, Caroline du Nord, Caroline du Sud, Colorado, Connecticut, Dakota du Nord, Dakota du Sud, Delaware, Floride, Hawaï, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiane, Maine, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, Nouveau Mexique, Ohio, Oklahoma, Oregon, Pennsylvanie, Rhodes Island, Tennessee, Texas, Utah, Vermont, Virginie, Virginie occidentale, Wisconsin et Wyoming. Les autres États adopteront probablement des textes d'application dans un proche avenir, dont l'Illinois, qui a déjà appliqué les dispositions de la Loi type de la CNUDCI par le biais de sa loi de 1998 relative à la sécurité du commerce électronique *(Electronic Commerce Security Act, 1998)*. On trouvera les dernières informations disponibles sur l'application de la loi uniforme à l'adresse: http://www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fsueta. asp (consulté le 6 juin 2008).

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

contrats internationaux (adoptée par l'Assemblée générale des Nations Unies dans sa résolution 60/21 du 23 novembre 2005 et ouverte à la signature le 16 janvier 2006) suivent la même approche, bien que la Loi type de la CNUDCI sur les signatures électroniques contienne quelques dispositions supplémentaires (voir le paragraphe 95 ci-dessous).

88. Lorsque la loi suit l'approche minimaliste, la question de savoir si l'équivalence de la signature électronique a été prouvée relève habituellement du pouvoir d'appréciation du juge, de l'arbitre ou de l'autorité publique, agissant généralement sur la base du "critère de fiabilité approprié". Selon ce principe, tous les types de signatures électroniques qui satisfont aux exigences sont considérés comme valables; le principe de neutralité technologique est donc inscrit dans ce critère.

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

2. Approche technospécifique

90. Le souci de promouvoir la neutralité technologique soulève d'autres questions importantes. L'impossibilité de garantir une sécurité absolue contre la fraude et les erreurs de transmission n'est pas limitée au monde du commerce électronique et s'applique aussi au monde des documents sur support papier. Lorsqu'ils sont appelés à formuler des règles en matière de commerce électronique, les législateurs sont fréquemment enclins à rechercher le degré de sécurité le plus élevé qu'offre la technologie existante[92]. Il n'est pas douteux que, dans la pratique, il faille appliquer les mesures de sécurité les plus rigoureuses

[92]L'un des premiers exemples a été la loi relative aux signatures numériques (Utah Digital Signature Act) promulguée par l'État de l'Utah, adoptée en 1995, mais abrogée à compter du 1er mai 2006 par l'ordonnance (State Bill) nº. 20 accessible sur le site Internet: http://www.le.state.ut.us/~2006/htmdoc/sbillhtm/sb0020.htm (consulté le 6 juin 2008). L'orientation technologique de la loi de l'Utah se retrouve dans un certain nombre de pays dont la législation ne reconnaît que les signatures numériques créées dans le cadre d'une ICP comme moyen valable d'authentification électronique, ce qui est le cas, par exemple, en Allemagne (Loi de 1997 relative aux signatures numériques, promulguée comme article 3 de la Loi relative aux services d'information et de communication du 13 juin 1997); en Argentine (*Ley de firma digital* (2001) et *Decreto* n° 2628/2002 (*Reglamentación de la Ley de firma digital*); en Estonie (Loi de 2000 relative aux signatures numériques); en Fédération de Russie (Loi de 2002 relative aux signatures électroniques); en Inde (*Information Technology Act, 2000*); en Israël (Loi de 2001 relative aux signatures électroniques); au Japon (Loi de 2001 relative aux signatures électroniques et aux services de certification); en Lituanie, (Loi de 2000 relative aux signatures électroniques); en Malaisie (Loi de 1997 relative aux signatures numériques); et en Pologne (Loi de 2001 relative aux signatures électroniques).

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

91. Les inconvénients de l'approche technospécifique sont qu'en privilégiant des types déterminés de signatures électroniques, elle "risque d'empêcher d'autres technologies éventuellement meilleures d'entrer en concurrence sur le marché"[93]. Plutôt que de faciliter le développement du commerce électronique et l'utilisation de techniques d'authentification électronique, une telle approche pourrait ainsi avoir l'effet opposé. En imposant une technologie déterminée, la législation risque de cristalliser des règles avant qu'une technologie déterminée ne parvienne à maturité[94]. Cette législation peut alors soit empêcher l'évolution ultérieure de la technologie en question, soit devenir rapidement obsolète par suite de l'évolution de la technique. Par ailleurs, toutes les applications n'exigent peut-être pas le même degré de sécurité que celui qu'offrent certaines techniques bien particulières, comme les signatures numériques. Il se peut également que la rapidité et la facilité des communications ou d'autres considérations soient plus importantes pour les parties que la nécessité de garantir l'intégrité de l'information électronique communiquée par tel ou tel moyen. Imposer l'utilisation de moyens d'authentification inutilement sûrs pourrait entraîner des gaspillages d'argent et d'efforts et ainsi entraver la diffusion du commerce électronique.

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

a) Autorégulation. Selon ce modèle, le domaine de l'authentification est laissé grand ouvert. Il se peut que l'État adopte pour sa propre administration plusieurs systèmes d'authentification, mais le secteur privé reste libre d'adopter les mécanismes

[93]Stewart Baker et Matthew Yeo, document d'information "Background and issues concerning authentication and the ITU" en collaboration avec le secrétariat de l'Union internationale des télécommunications, présenté à la réunion d'experts sur les signatures électroniques et les autorités de certification: incidences pour les télécommunications, Genève, 9 et 10 décembre 1999, document n° 2, accessible sur le site Internet: www.itu.int/osg/spu/ni/esca/meetingdec9-101999/briefingpaper.html (consulté le 6 juin 2008).

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

d'authentification, commerciaux ou autres, qu'il juge appropriés. Il n'est pas désigné d'autorité supérieure de l'authentification, et les prestataires de services d'authentification ont la responsabilité d'assurer l'interopérabilité avec les autres prestataires de services nationaux et internationaux, selon les objectifs du système d'authentification. Aucune licence ni agrément technologique ne sont exigés des prestataires de service d'authentification (sous réserve, le cas échéant, de règlements relatifs à la protection des consommateurs)[95];

b) Participation limitée des pouvoirs publics. L'État peut décider d'établir une autorité supérieure d'authentification, volontairement acceptée ou obligatoire. En pareil cas, les prestataires de service d'authentification pourront se trouver dans la nécessité d'entrer en rapport avec ladite autorité pour que leurs marques d'authentification (ou autres authentificateurs) soient acceptées en dehors de leurs propres systèmes. Les spécifications techniques et les modalités de gestion des prestataires de service d'authentification devront alors être publiées aussi rapidement que possible de sorte que les services publics, tout comme le secteur privé, puissent s'organiser en conséquence. Les prestataires de services d'authentification peuvent également être sujets à des licences ou agrément technologiques[96];

c) Mécanisme public. Il se peut que l'État décide de créer un prestataire de services d'authentification central, à compétence exclusive. Des prestataires de service d'authentification à des fins spéciales peuvent également être établis avec l'autorisation de l'État[97]. Les systèmes de gestion de l'identité (voir paragraphes 67 à 77 ci-dessus) constituent pour l'État un autre moyen de diriger indirectement le processus de signature numérique. Quelques pays ont déjà lancé des programmes en vue de délivrer à la population des documents d'identité à lecture automatique dotés de fonctionnalités de signatures numériques "identifications électroniques".

3. Approche dualiste

93. Selon cette approche, la loi fixe un seuil minimum de conditions auxquelles doivent répondre les méthodes d'authentification électronique pour avoir un certain statut juridique minimum, et accorde un effet juridique plus large à certaines méthodes d'authentification électronique (parfois appelées signatures électroniques sécurisées, avancées ou renforcées ou bien à certificats qualifiés)[98]. Au niveau le plus élémentaire, les législations qui reposent sur une approche dualiste reconnaissent généralement aux signatures électroniques l'équivalence fonctionnelle des signatures manuscrites sur la base de critères technologiquement neutres. Des signatures reflétant un niveau de sécurité plus élevé, auquel s'appliquent certaines présomptions réfutables, sont nécessaires dans des conditions spécifiques liées éventuellement à l'utilisation d'une

[95]Coopération économique Asie-Pacifique (APEC). *Assessment Report on Paperless Trading of APEC Economies* (Beijing, secrétariat de l'APEC, 2005), pages 63 et 64, où les États-Unis sont cités comme exemple d'application de ce modèle.

[96]Voir Coopération économique Asie-Pacifique (APEC), *Assessment Report* …, où Singapour est cité comme exemple.

[97]Voir Coopération économique Asie-Pacifique (APEC), *Assessment Report* …, où la Chine et la Malaisie sont citées comme exemples.

[98]Aalberts et van der Hof, *Digital Signature Blindness* …, paragraphe 3.2.2.

technologie déterminée. À l'heure actuelle, les législations de ce type définissent habituellement de telles signatures sécurisées sur la base des technologies ICP.

94. Cette approche est habituellement celle qui est retenue par les pays qui considèrent que leur législation doit fixer un certain nombre de normes technologiques tout en laissant libre cours aux progrès de la technologie. Elle peut offrir un moyen terme entre flexibilité et certitude en matière de signatures électroniques, en laissant aux parties le soin de décider, à la lumière de leurs usages commerciaux, si le coût et la gêne que suppose l'utilisation d'une méthode plus sûre sont justifiés par leurs besoins. Ces textes donnent également des indications concernant les critères de reconnaissance des signatures électroniques pour ce qui est du modèle d'autorité de certification. Il est généralement possible de combiner l'approche dualiste et n'importe quel type de modèle de certification (autorégulation, accréditation volontaire ou mécanisme public), de façon largement ressemblante à ce qui peut être fait dans l'approche technospécifique (voir plus haut, paragraphes 90 à 92). Ainsi, si certaines règles peuvent être suffisamment flexibles pour rendre possible l'utilisation de différents modèles de certification des signatures électroniques, certains systèmes ne reconnaissent que les prestataires de services de certification agréés comme émetteurs possibles de certificats sécurisés ou qualifiés.

95. Les premiers à adopter des textes reposant sur l'approche dualiste ont notamment été Singapour[99] et l'Union européenne[100]. Plusieurs autres pays ont suivi[101]. La

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

[100] Comme la loi singapourienne relative aux transactions électroniques, la directive de l'Union européenne sur les signatures électroniques (*Journal officiel des Communautés européennes*, L 13/12, 19 janvier 2000) établit une distinction entre la "signature électronique" (définie au paragraphe 1 de l'article 2 comme étant "une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification") et la "signature électronique avancée" (définie au paragraphe 2) dudit article comme étant une signature électronique satisfaisant aux exigences suivantes: "*a)* être liée uniquement au signataire, *b)* permettre d'identifier le signataire, *c)* être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, et *d)* être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable". Aux termes du paragraphe 2 de l'article 5 de la directive, les États membres de l'UE doivent veiller à ce que "l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique" au seul motif que "la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature". Cependant, seules les signatures électroniques avancées "basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature" sont considérées comme répondant "aux exigences légales d'une signature à l'égard de données électroniques, de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites imprimées sur papier" et étant "recevables comme preuves en justice" (voir paragraphe 1 de l'article 5 de la directive).

[101] Par exemple Maurice et Pakistan. Pour de plus amples détails sur les législations respectives, voir la note 88 ci-dessus.

Loi type de la CNUDCI sur les signatures électroniques permet à l'État ayant décidé d'appliquer ce texte de mettre en place un système dualiste, même si elle ne l'encourage pas activement[102].

96. S'agissant du deuxième niveau, il a été proposé que les pays n'exigent pas l'utilisation de signatures du deuxième niveau dans le cas des conditions de forme des transactions commerciales internationales et que les signatures électroniques sécurisées soient limitées aux domaines d'application du droit qui n'ont guère d'impact sur le commerce international (par exemple fiducie, droit de la famille, transactions immobilières)[103]. Il a été suggéré en outre que les lois envisageant deux niveaux de signatures reconnaissent expressément l'effet des accords contractuels touchant l'utilisation de la reconnaissance des signatures électroniques, pour que les modèles mondiaux d'authentification de type contractuel n'aillent pas à l'encontre des réglementations nationales.

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

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

1. "Authentification" et attribution des enregistrements électroniques

98. L'utilisation de méthodes électroniques d'identification soulève deux questions qui méritent d'être examinées ici. La première a trait à celle, générale, de l'attribution d'un message à son expéditeur supposé. La seconde est de savoir si la méthode

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

[103]Baker et Yeo, "Background and issues concerning authentication…".

d'identification utilisée par les parties est propre à satisfaire aux conditions de forme, en particulier les conditions légales de signature. Une attention particulière doit également être accordée aux notions juridiques qui impliquent l'existence d'une signature manuscrite, par exemple la notion de "document" dans certains systèmes juridiques. Même si ces deux questions sont souvent imbriquées voire, selon les circonstances, impossibles à dissocier complètement, il peut être utile de tenter de les analyser séparément car les juridictions parviennent apparemment à des conclusions différentes suivant la fonction attribuée à la méthode d'authentification.

99. La Loi type sur le commerce électronique traite de l'attribution des messages de données dans son article 13. Cette disposition tire son origine de l'article 5 de la Loi type de la CNUDCI sur les virements internationaux[104], qui définit les obligations de l'expéditeur d'un ordre de paiement. L'article 13 est censé s'appliquer lorsque se pose la question de savoir si un message de données a réellement été envoyé par la personne qui est désignée comme l'expéditeur. Dans le cas d'une communication sur papier, le problème se poserait lorsque la signature de l'expéditeur présumé semblerait avoir été contrefaite. Dans un environnement électronique, il se peut qu'une personne non autorisée ait envoyé le message, l'authentification par codage, cryptage ou toute autre méthode par ailleurs correcte. L'article 13 n'a pas pour objet d'attribuer la paternité d'un message de données ou d'établir l'identité des parties. Il traite plutôt de l'attribution des messages de données en établissant les conditions dans lesquelles une partie peut se fier à la présomption selon qu'un message de données émanait véritablement de l'expéditeur supposé.

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

101. Un certain nombre de pays ont adopté la règle énoncée à l'article 13 de la Loi type, y compris la présomption d'attribution établie au paragraphe 3 de cet article[105]. La législation de certains pays considère expressément l'utilisation de codes, de mots de passe ou d'autres moyens d'identification comme des facteurs créant une présomption de paternité du message[106]. Il existe également des versions plus générales de l'article 13, dans lesquelles la présomption créée par une vérification correcte à l'aide

[104]Publication des Nations Unies, numéro de vente: F.99.C.11, accessible sur le site Internet: http://www.uncitral.org/pdf/english/texts/payments/transfers/ml-credittrans.pdf (consulté le 6 juin 2008).

[105]Colombie (article 17); Équateur (article 10); Jordanie (article 15); Maurice (paragraphe 2 de l'article 12); Philippines (paragraphe 3 de l'article 18); République de Corée (paragraphe 2 de l'article 7); Singapour (paragraphe 3 de l'article 13); Thaïlande (article 16) et Venezuela (République bolivarienne du) (article 9). On trouve des règles semblables dans la législation de Jersey (dépendance de la Couronne britannique) (article 8) et des territoires britanniques d'outre-mer des Bermudes (paragraphe 2 de l'article 16) et des îles Turques et Caïques (article 14). Pour de plus amples détails, voir note 88 ci-dessus.

[106]Mexique (voir note 88 ci-dessus), paragraphe I de l'article 90.

d'une procédure précédemment convenue est reformulée en tant qu'indication des éléments pouvant être utilisés à des fins d'attribution du message[107].

102. D'autres pays n'ont adopté que les règles générales de l'article 13 de la Loi type, à savoir qu'un message de données émane de l'expéditeur s'il a été envoyé par l'expéditeur lui-même ou par une personne agissant en son nom, ou encore par un système programmé par l'expéditeur ou en son nom pour fonctionner automatiquement[108]. Enfin, quelques pays qui ont incorporé la Loi type sur le commerce électronique dans leur droit interne n'ont pas prévu de dispositions particulières fondées sur l'article 13[109]. Ces pays sont partis du principe qu'aucune règle particulière n'était nécessaire et qu'il valait mieux utiliser les mêmes moyens de preuve ordinaire pour l'attribution des messages que pour l'attribution de documents sur papier: "Celui qui désire invoquer une signature s'expose toujours à ce que celle-ci soit invalide. La règle demeure la même dans le cas des signatures électroniques"[110].

103. D'autres pays ont néanmoins préféré séparer les dispositions de la Loi type sur le commerce électronique concernant l'attribution de celles qui ont trait aux signatures électroniques. Cette approche est basée sur l'idée que, dans un contexte documentaire, l'attribution a essentiellement pour objectif de constituer une présomption raisonnable et peut reposer sur des moyens plus larges que ceux qui servent exclusivement à identifier une personne. Les législations de certains pays, comme la loi uniforme des États-Unis relative aux transactions électroniques, mettent en relief ce principe en stipulant, par exemple, qu'"un enregistrement électronique ou une signature électronique peut être attribué à une personne si cet enregistrement ou cette signature était l'acte de cette personne", ce qui "peut être prouvé par tout moyen, y compris par la démonstration de l'efficacité de toute procédure de sécurité appliquée pour déterminer à qui l'enregistrement électronique ou la signature électronique était attribuable"[111].

---

[107]Par exemple, la Loi uniforme des États-Unis relative aux opérations électroniques (UETA) (voir note 90) prévoit, au paragraphe *a)* de son article 9, qu'un enregistrement électronique ou une signature électronique "peut être attribué à une personne si cet enregistrement ou cette signature était un acte de cette personne. L'acte de la personne peut être prouvé par tout moyen, y compris par la démonstration de l'efficacité de toute procédure de sécurité appliquée, pour déterminer à qui l'enregistrement électronique ou la signature électronique était imputable". Le paragraphe *b)* de l'article 9 dispose en outre que l'effet d'un enregistrement électronique ou d'une signature électronique attribué à une personne en vertu du paragraphe *a)* "est déterminé à partir du contexte et des circonstances au moment de sa création, de son exécution ou son adoption, y compris toute convention éventuelle des parties, et de toute autre manière prévue par la loi".

[108]Australie (paragraphe 1 de l'article 15); des règles essentiellement identiques sont inscrites dans la législation des pays suivants: Inde (article 11); Pakistan (paragraphe 2 de l'article 13); Slovénie (article 5). Voir aussi Région administrative spéciale (SAR) chinoise de Hong Kong (article 18) et île de Man (dépendance de la Couronne britannique) (article 2). Pour de plus amples détails sur les lois concernées, voir note 88 ci-dessus.

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

[110]Canada, Loi uniforme annotée sur le commerce électronique (voir note 88), commentaire officiel de l'article 10.

[111]États-Unis, Loi uniforme de 1999 relative aux transactions électroniques (voir note 90, article 9). Le paragraphe 1 du commentaire officiel de l'article 9 offre les exemples suivants d'attribution à une personne, aussi bien de l'enregistrement que d'une signature électronique: la personne "tape son nom dans une commande par courrier électronique"; "l'employé de la personne, conformément au pouvoir qui lui a été donné, tape le nom de la personne dans une commande par courrier électronique"; ou "l'ordinateur de la personne, programmé pour commander des biens sur réception d'informations concernant les stocks suivant des paramètres particuliers, émet une commande dans laquelle figure le nom de la personne ou d'autres informations identifiantes".

Cette règle générale d'attribution n'affecte pas l'utilisation d'une signature comme moyen d'attribuer un enregistrement à une personne mais est fondée sur l'admission qu'"une signature n'est pas la seule méthode d'attribution"[112]. Selon le commentaire officiel de cette loi, par conséquent:

> "4. Un environnement électronique peut contenir certaines informations qui ne semblent pas attribuer un enregistrement particulier à une personne ou qui établissent un lien clair entre cette personne et cet enregistrement. Les codes numériques, les numéros d'identification personnels et les combinaisons de clefs publiques et privées servent à établir à quelle partie un enregistrement électronique devrait être attribué. Bien évidemment, les procédures de sécurité seront un autre élément de preuve en matière d'attribution.
>
> La mention expresse des procédures de sécurité en tant que moyen de prouver l'attribution d'un enregistrement est salutaire en raison de l'importance capitale de ce type de procédure dans l'environnement électronique. Dans certains cas, une procédure technique et technologique de sécurité peut être le meilleur moyen de convaincre un juge que tel ou tel enregistrement ou signature électronique est le fait d'une personne déterminée. Dans certaines circonstances, l'utilisation d'une procédure de sécurité pour établir qu'un enregistrement et la signature s'y rattachant proviennent de l'entreprise de la personne sera peut-être nécessaire pour réfuter une allégation de piratage informatique. La mention des procédures de sécurité ne veut pas dire que d'autres formes de preuves devraient se voir attribuer un effet persuasif moindre. Il importe aussi de rappeler que la valeur particulière d'une procédure donnée n'a pas d'incidence sur son caractère même de procédure de sécurité mais influe seulement sur le poids à lui accorder en tant que preuve tendant à fixer l'attribution"[113].

104. Il est important également de ne pas perdre de vue qu'une présomption d'attribution ne se substituerait pas à l'application des règles de droit sur les signatures lorsqu'une signature est nécessaire pour valider ou prouver un acte. Lorsqu'il est établi qu'un enregistrement ou une signature est attribuable à une partie, "l'effet d'un enregistrement ou d'une signature doit être déterminé à la lumière du contexte et des circonstances, y compris toute convention éventuelle des parties", ainsi qu'en fonction "d'autres conditions légales envisagées à la lumière de ce contexte"[114].

---

[112]Ibid. Le paragraphe 3 du commentaire officiel de l'article 9 se lit comme suit : "L'utilisation de la transmission par télécopie fournit plusieurs exemples d'attribution à partir d'informations autres qu'une signature. Une télécopie peut être attribuée à une personne en raison des informations imprimées en haut de la page, qui indiquent la machine à partir de laquelle elle été envoyée. De même, le document transmis peut contenir un en-tête qui identifie l'expéditeur. Dans certaines décisions, cet en-tête a été considéré comme constituant effectivement une signature parce qu'il s'agissait d'un symbole adopté par l'expéditeur dans l'intention d'identifier la télécopie. Toutefois, la détermination de la signature découlait de la nécessité d'établir l'intention en l'espèce. Dans d'autres décisions, les en-têtes de télécopies n'ont PAS été considérés comme des signatures car l'intention requise était absente. L'important est qu'avec ou sans signature, l'information contenue dans l'enregistrement électronique sera très probablement suffisante pour fournir les éléments conduisant à l'attribution d'un enregistrement électronique à une partie déterminée".

[113]Commentaire officiel sur l'article 9.

[114]Paragraphe 6 du commentaire officiel sur l'article 9.

105. S'appuyant sur cette conception flexible de l'attribution, les tribunaux des États-Unis semblent faire preuve de souplesse en ce qui concerne la recevabilité des enregistrements électroniques, y compris des courriels, comme élément de preuve en matière civile[115]. Des tribunaux américains ont rejeté les arguments selon lesquels les messages électroniques n'étaient pas recevables du fait qu'ils n'étaient pas authentifiés et constituaient une preuve testimoniale[116]. Ils ont estimé au contraire que les courriels reçus du demandeur pendant la procédure de divulgation des pièces s'authentifiaient eux-mêmes car "la production pendant la procédure de divulgation de documents détenus par les parties est un motif suffisant pour considérer ces documents comme s'auto-authentifiant"[117]. Les tribunaux prennent généralement en considération tous les éléments de preuve disponibles et ne rejettent pas les enregistrements électroniques comme étant en principe irrecevables.

106. Dans les pays qui n'ont pas adopté la Loi type sur le commerce électronique, la législation ne contient apparemment pas de dispositions particulières traitant de l'attribution des messages d'une manière similaire. Dans ces pays, l'attribution dépend généralement de la reconnaissance juridique des signatures électroniques et des présomptions associées aux enregistrements authentifiés par des types particuliers de signatures électroniques. Les craintes exprimées au sujet du risque de manipulation des enregistrements électroniques, par exemple, ont conduit les tribunaux de certains de ces pays à refuser de considérer les courriels comme des éléments de preuve recevables, au motif que les courriels ne comportent de garanties suffisantes d'intégrité[118]. Il existe aussi d'autres exemples de cette approche plus restrictive en matière de valeur probante des enregistrements et attributions électroniques dans plusieurs affaires récentes de ventes aux enchères sur Internet, pour lesquelles les tribunaux ont appliqué une règle stricte en matière d'attribution des messages de données. Ces affaires concernaient le plus souvent des allégations de contravention au contrat, fondées sur le défaut de paiement de biens prétendument achetés aux enchères sur Internet. Les demandeurs soutenaient chaque fois que les défendeurs étaient l'acheteur, étant donné que l'offre la plus élevée avait été authentifiée par le mot de passe du défendeur et avait été envoyée depuis l'adresse électronique de ce dernier. Les tribunaux ont estimé que ces éléments n'étaient pas suffisants pour conclure avec certitude que le défendeur avait bien participé à la vente aux enchères et soumis l'offre retenue. Ils ont invoqué divers arguments pour justifier cette position. Par exemple, les mots de passe n'étaient pas fiables car toute personne connaissant le mot de passe du défendeur aurait pu utiliser l'adresse électronique de ce dernier depuis n'importe où et participer à la

---

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

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

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

[118]Allemagne, Amtsgericht (Tribunal de district) Bonn, Affaire n° 3 C 193/01, 25 octobre 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC WebDok 332/2002, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20020332.htm (consulté le 6 juin 2008).

vente aux enchères en se servant de son nom[119], un risque jugé très élevé par certains tribunaux au vu des avis d'experts concernant des menaces d'atteinte à la sécurité des réseaux de communication par Internet, en particulier du fait de l'utilisation de chevaux de Troie permettant de "voler" le mot de passe d'une personne[120]. Le risque d'une utilisation non autorisée d'un mode d'identification (mot de passe) devait être supporté par la partie qui offrait les biens ou services par un moyen particulier, faute de présomption légale selon laquelle les messages envoyés par l'intermédiaire d'un site web sur l'Internet à l'aide du mot de passe d'une personne permettant d'accéder à ce site étaient attribuables à cette personne[121]. Une telle présomption pouvait éventuellement être attachée à une "signature électronique avancée" telle que définie par la loi, mais le détenteur d'un mot de passe ne devait pas assumer le risque que celui-ci soit détourné par des personnes non autorisées[122].

2. Capacité à satisfaire les exigences légales concernant les signatures

107. Dans certains pays, les tribunaux ont été enclins à interpréter de façon souple les exigences légales en matière de signature. Comme indiqué plus haut (voir Introduction, paragraphes 2 à 4), tel a été le cas généralement dans certains pays de *common law* relativement à des dispositions des lois antifraudes qui stipulent que certaines transactions, pour être valables, doivent être établies par écrit et porter une signature. Aux États-Unis, des tribunaux ont également accueilli favorablement la reconnaissance par le législateur des signatures électroniques, admettant leur utilisation dans des situations qui n'étaient pas expressément prévues dans la loi d'habilitation, par exemple dans le cas des mandats judiciaires[123].Fait plus important pour le domaine contractuel, les tribunaux ont également déterminé si l'identification était adéquate en tenant compte des transactions entre les parties plutôt qu'en recourant à une règle stricte pour toutes les situations. Ainsi, lorsque les parties avaient régulièrement utilisé des courriels dans leurs négociations, les tribunaux ont estimé que le nom dactylographié de l'expéditeur figurant dans un message électronique satisfaisait à l'exigence légale de signature[124]. Le choix délibéré

---

[119]Allemagne, Amtsgericht (Tribunal de district) Erfurt, Affaire n° 28 C 2354/01, 14 septembre 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 71/2002, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20020071.htm (consulté le 6 juin 2008); voir aussi Landesgericht (Tribunal du Land) Bonn, Affaire n° 2 O 472/03, 19 décembre 2003, *JurPC, Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 74/2004, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20040074.htm (consulté le 6 juin 2008).

[120]Allemagne, Landesgericht (Tribunal du Land) Konstanz, Affaire n° 2 O 141/01 A, 19 avril 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 291/2002, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20020291.htm (consulté le 6 juin 2008).

[121]Allemagne, Landesgericht (Tribunal du Land) Bonn, Affaire n° 2 O 450/00, 7 août 2001, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 136/2002, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20020136.htm (consulté le 6 juin 2008).

[122]Allemagne, Oberlandesgericht (Court of Appeal) Köln, Affaire n° 19 U 16/02, 6 septembre 2002, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 364/2002, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20020364.htm (consulté le 6 juin 2008).

[123]*Department of Agriculture and Consumer Services* c. *Haire*, Fourth District Court of Appeal of Florida, Affaires n° 4D02-2584 et 4D02-3315, 15 janvier 2003.

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

d'une personne de dactylographier son nom à la fin de tous ses courriels a été considéré comme une authentification valable[125]. Le fait que les tribunaux américains se montrent disposés à considérer que les courriels et les noms qui y sont dactylographiés peuvent satisfaire aux exigences de l'écrit[126] reflète une interprétation extensive de la notion de "signature", qui est entendue comme englobant "tout symbole apposé ou adopté par une partie dans l'intention d'authentifier un écrit" de sorte que, dans certains cas, "un nom dactylographié ou un en-tête sur un document suffit à satisfaire à l'exigence de signature"[127]. Lorsque les parties ne contestent pas avoir expédié ou reçu des communications par courriel, les exigences légales de signature se trouveraient satisfaites étant donné que les tribunaux reconnaissent "depuis longtemps qu'une signature liant son auteur peut revêtir la forme de toute marque ou désignation jugée appropriée par la partie en question", dans la mesure où celle-ci "a l'intention de s'engager"[128].

108. Les tribunaux britanniques ont suivi une démarche semblable, considérant généralement la forme d'une signature comme moins importante que sa fonction. Ainsi, les tribunaux tiennent compte habituellement de l'adéquation du moyen utilisé aussi bien pour attribuer un message à une personne déterminée que pour indiquer l'intention de la personne en ce qui concerne le message. Les courriels peuvent par conséquent constituer des "documents" et les noms saisis dans ceux-ci être des "signatures"[129]. Quelques tribunaux ont déclaré n'avoir "aucun doute que si une partie crée et expédie un message électronique, elle sera considérée comme l'ayant signé tout comme si elle avait apposé sa signature manuscrite sur le même document sur papier" et que "le fait que le document est créé électroniquement plutôt que sur un support papier ne peut faire aucune différence"[130]. À l'occasion, des tribunaux ont refusé d'admettre, dans le contexte de la législation antifraude, qu'un courriel constituait un contrat signé, essentiellement parce que l'intention des parties d'être liées par la signature faisait défaut. Cependant, il ne paraît pas y avoir de cas dans lequel les tribunaux ont refusé a priori de considérer qu'un courriel et les noms qui y étaient dactylographiés pouvaient satisfaire aux exigences légales en matière d'écrit et de signature. Dans certains cas, les tribunaux ont considéré que les conditions fixées par la législation anti-fraude n'étaient pas satisfaites car les courriels en question reflétaient simplement les négociations en cours et non un accord final, par exemple parce que, lors des négociations, l'intention

[125] *Jonathan P. Shattuck* c. *David K. Klotzbach*, Superior Court of Massachusetts, 11 décembre 2001, 2001 Mass. Super. LEXIS 642.

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

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

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

[129] *Hall* c. *Cognos Limited* (Hull Industrial Tribunal, Affaire n° 1803325/97) (non publiée).

[130] *Mehta* c. *J. Pereira Fernandes S.A.* [2006] EWHC 813 (Ch), (United Kingdom, England and Wales High Court, Chancery Division), [2006] 2 Lloyd's Rep 244 (Royaume-Uni, Angleterre et Pays de Galles, Lloyd's List Law Reports).

de l'une des parties était qu'un contrat liant l'une et l'autre serait conclu après la signature d'un "mémorandum d'accord" et pas avant[131]. Dans d'autres cas, des tribunaux ont fait savoir qu'ils auraient peut-être été enclins à admettre comme signature "le nom ou les initiales" de son auteur "à la fin du courriel" ou "en tout autre endroit dans le corps même du courriel", considérant cependant que "l'insertion automatique de l'adresse électronique d'une personne après que le document a été transmis par le prestataire de services Internet d'expédition et/ou de réception n'était pas "censée constituer une signature"[132]. Bien que les tribunaux britanniques paraissent interpréter les dispositions de la législation anti-fraude concernant l'exigence d'un écrit plus rigoureusement que leurs homologues américains, ils tendent généralement à admettre l'utilisation de tout type de signature électronique ou de méthode d'authentification, même en l'absence d'autorisation expresse du législateur, aussi longtemps que la méthode en question remplit les mêmes fonctions qu'une signature manuscrite[133].

109. Dans les pays de droit romain, les tribunaux ont généralement tendance à suivre une approche plus restrictive, sans doute parce que, pour beaucoup de ces pays, la notion de "document" implique d'ordinaire l'usage d'une forme ou d'une autre d'authentification, ce qui le rend difficile à distinguer d'une "signature". Dans des pays comme la France, par exemple, des tribunaux ont hésité à accepter les moyens électroniques d'identification comme équivalant à une signature manuscrite avant l'adoption d'une législation reconnaissant expressément la validité des signatures électroniques[134]. Une approche un peu plus souple, cependant, se reflète dans un certain nombre de décisions judiciaires qui ont accepté le dépôt par voie électronique de plaintes administratives pour respecter un délai fixé par la loi, du moins à condition que ces plaintes soient ensuite confirmées par courrier ordinaire[135].

110. Alors qu'elles ont adopté une approche restrictive pour l'attribution des messages de données dans la formation des contrats, les juridictions allemandes ont fait preuve de souplesse dans la reconnaissance des méthodes d'acceptation comme équivalant aux

---

[131] *Pretty Pictures Sarl* c. *Quixote Films Ltd*., 30 janvier 2003 ([2003] EWHC 311 (QB), [United Kingdom, England and Wales High Court, Law Reports Queen's Bench, [2003] All ER (D) 303 (January)] [Royaume-Uni, All England Direct Law Reports (Digests)].

[132] *Mehta* c. *J. Pereira Fernandes S.A.* …(voir note 130).

[133] *Mehta* c. *J. Pereira Fernandes S.A.* n° 25: "Il faut noter que la Commission des lois estime, relativement à la [directive de l'Union européenne sur le commerce électronique (2000/31/EC)], qu'il n'y a pas lieu d'apporter de modifications significatives aux lois qui exigent une signature, car la question de savoir si les exigences prévues par lesdites lois ont été satisfaites peut être réglée de manière fonctionnelle en se demandant si la conduite du signataire apparent reflète, pour une personne raisonnable, une intention d'authentifier le message. […] Ainsi, comme je l'ai déjà dit, si une partie ou l'agent d'une partie qui expédie un courriel et dactylographie son nom ou le nom de son mandant comme exigé ou autorisé par la jurisprudence dans le corps même d'un courriel, cela constituerait à mon avis une signature suffisante aux fins de la [Loi relative à la fraude]."

[134] La Cour de cassation française a jugé irrecevable une requête en appel signée électroniquement, attendu qu'il existait des doutes sur l'identité de la personne ayant créé la signature et que la requête avait été signée électroniquement avant l'entrée en vigueur de la loi du 13 mars 2000 reconnaissant l'effet juridique des signatures électroniques [Cour de cassation, 2e chambre civile, 30 avril 2003, *Société Chalets Boisson* c. *M. X.*, accessible sur le site Internet à l'adresse: www.juriscom.net/jpt/visu.php?ID=239 (consulté le 6 juin 2008)].

[135] France, Conseil d'État, 28 décembre 2001, n° 235784, *Élections municipales d'Entre-Deux-Monts* (original disponible au secrétariat).

signatures manuscrites dans le cadre de procédures judiciaires. En Allemagne, le débat a porté sur l'utilisation de plus en plus fréquente d'images numérisées de la signature d'un avocat pour identifier des télécopies numérisées contenant des déclarations d'appels, transmises directement par modem depuis l'ordinateur à un télécopieur d'un tribunal. Dans les premières affaires jugées, les cours d'appel[136] et la Cour fédérale de justice[137] avaient estimé qu'une image numérisée d'une signature manuscrite ne satisfaisait pas aux exigences en matière de signature et ne prouvait pas l'identité d'une personne. Une fonction d'identification pouvait éventuellement être attribuée à une "signature électronique avancée", telle que définie dans la législation allemande. Toutefois, il incombait généralement au législateur et non au juge d'établir les conditions d'équivalence entre les écrits et les communications dématérialisés par transferts de données[138]. Cette interprétation a finalement été infirmée en raison de l'opinion unanime des autres cours fédérales supérieures qui ont accepté la remise de certaines pièces de procédure par communication électronique d'un message de données contenant l'image numérisée d'une signature[139].

111. Il est intéressant de noter que même les tribunaux de certains pays de droit romain qui ont promulgué une législation reconnaissant l'utilisation de signatures numériques basées sur l'infrastructure à clef publique, comme la Colombie[140], ont adopté une approche souple et ont confirmé, par exemple, qu'une procédure judiciaire pouvait être menée entièrement au moyen de communications électroniques. Les pièces échangées pendant une telle procédure étaient valables même si elles n'étaient pas revêtues d'une signature numérique, étant donné que les communications électroniques utilisaient des méthodes permettant d'identifier les parties[141].

---

[136]Par exemple, Oberlandesgericht (Cour d'appel) Karlsruhe, Affaire n° 14 U 202/96, 14 novembre 1997, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 09/1998, accessible sur le site Internet: http://www.jurpc.de/rechtspr/19980009.htm (consulté le 6 juin 2008).

[137]Allemagne, Bundesgerichtshof (Cour fédérale de justice), Affaire n° XI ZR 367/97, 29 septembre 1998, *JurPC Internet-Zeitschrift für Rechtsinformatik und Informationsrecht*, JurPC Web-Dok. No. 05/1999, accessible sur le site Internet: http://www.jurpc.de/rechtspr/19990005.htm (consulté le 6 juin 2008).

[138]Ibid.

[139]Dans une décision rendue au sujet d'une affaire que lui avait soumise la Cour fédérale de justice, la Chambre commune des cours suprêmes fédérales d'Allemagne a noté que les conditions de forme dans les procédures judiciaires n'étaient pas une fin en soi. Leur but était d'assurer une détermination suffisamment fiable du contenu de l'écrit et de l'identité de la personne dont émanait cet écrit. La Chambre commune a constaté que l'application dans la pratique des conditions de forme avait évolué de manière à tenir compte des récentes innovations technologiques, telles que le télex ou la télécopie. Elle a estimé que l'acceptation de la remise de certaines pièces de procédure par communication électronique d'un message de données contenant une image numérisée d'une signature serait conforme à l'esprit de la jurisprudence existante (Gemeinsamer Senat der obersten Gerichtshöfe des Bundes, GmSOGB 1/98, 5 avril 2000, *JurPC Internet Zeitschrift für Rechtsinformatik*, JurPC WebDok 160/2000, accessible sur le site Internet: http://www.jurpc.de/rechtspr/20000160.htm (consulté le 6 juin 2008).

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

[141]Colombie, Juzgado Segundo Promiscuo Municipal Rovira Tolima, *Juan Carlos Samper* c. *Jaime Tapias*, 21 juillet 2003, Rad. 73-624-40-89-002-2003-053-00. Le tribunal a considéré que la procédure menée par les moyens électroniques était valable alors même que les courriels n'étaient pas revêtus d'une signature juridique étant donné: *a)* que l'expéditeur des messages de données pouvait être pleinement identifié; *b)* que l'expéditeur des messages de données avait accepté et confirmé le contenu du message envoyé; *c)* que les messages de données étaient conservés en lieu sûr au Tribunal; et *d)* que les messages pouvaient être examinés à tout moment, accessible sur le site Internet: http://www.camara-e.net/_upload/80403--0-7-diaz082003.pdf (consulté le 6 juin 2008).

112. La jurisprudence concernant les signatures électroniques demeure rare et les quelques décisions judiciaires rendues jusqu'à présent ne constituent pas une base suffisante pour tirer des conclusions fermes. Néanmoins, un bref examen des précédents existants fait apparaître plusieurs tendances. Il semble que l'approche adoptée par le législateur en matière de signatures électroniques et d'authentification ait influencé l'attitude des tribunaux dans ce domaine. L'accent mis par le législateur sur les "signatures" électroniques, en l'absence de règle générale concomitante d'attribution, a peut-être conduit à accorder une attention excessive à la fonction d'identification des méthodes d'authentification. Il en est résulté dans certains pays quelque méfiance à l'égard des méthodes d'authentification qui ne répondent pas à la définition légale d'une "signature" électronique. Il n'est pas dit que ces mêmes tribunaux, ayant adopté une approche souple dans le cadre de procédures d'appel judiciaires ou administratives, le seraient autant devant les conditions de signatures nécessaires à la validité des contrats. En effet, si dans un contexte contractuel une partie s'expose au risque de voir l'accord rejeté par l'autre partie, dans une procédure civile, c'est généralement la partie utilisant une signature ou un enregistrement électronique qui souhaite confirmer qu'elle approuve l'enregistrement et son contenu.

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

a) Applications internationales: apostilles électroniques

113. Une commission spéciale s'est réunie à La Haye du 28 octobre au 4 novembre 2003 pour examiner le fonctionnement pratique de la Convention supprimant l'exigence de la légalisation des actes publics étrangers (Convention apostille de La Haye), de la Convention relative à la signification et à la notification à l'étranger des actes judiciaires et extrajudiciaires en matière civile ou commerciale, de la Convention relative à la signification et la notification à l'étranger des actes judiciaires et extrajudiciaires en matière civile ou commerciale[142] et de la Convention sur l'obtention des preuves à l'étranger en matière civile ou commerciale[143]. La réunion de la commission spéciale sur le fonctionnement pratique des conventions Apostille, Obtention des preuves et Notification a accueilli 116 délégués représentant 57 États membres, États parties à une ou plusieurs des Conventions examinées, et observateurs. La Commission spéciale a souligné que les trois conventions fonctionnaient dans un environnement soumis à des mouvements technologiques d'envergure. Cette évolution ne pouvait certes pas être prévisible à l'époque de l'adoption des trois conventions, mais la Commission spéciale a souligné que les technologies modernes constituaient désormais une part intégrante de la société moderne actuelle et que leur usage était un élément de fait[144]. À cet égard, la Commission spéciale à noté que l'esprit et la lettre de ces Conven-

[142]Nations Unies, *Recueil des Traités*, vol. 658, nº. 9432.

[143]Ibid., vol. 847, nº. 12140.

[144]Conférence de La Haye de droit international privé "Conclusions et recommandations adoptées par la commission spéciale sur le fonctionnement pratique des conventions Apostille de La Haye, Obtention des preuves et Notification, 28 octobre au 4 novembre 2003" (accessible sur le site Internet: http://hcch.e-vision.nl/upload/wop/lse_concl_e.pdf, 6 juin 2008).

tions ne constituent pas un obstacle à l'utilisation des technologies modernes et que leurs applications et leur fonctionnement peuvent être davantage améliorés par l'utilisation de telles techniques[145]. La Commission spéciale a recommandé que les États parties aux conventions et le Bureau permanent de la Conférence de La Haye de droit international privé travaillent au développement de techniques de production d'apostilles électroniques "tenant compte, entre autres des lois types de la CNUDCI sur le commerce électronique et les signatures électroniques, toutes deux fondées sur les principes de non-discrimination et d'équivalence fonctionnelle"[146]. En avril 2006, le Bureau permanent de la Conférence de La Haye de droit international privé et l'Association nationale des notaires (National Notary Association, NNA) des États-Unis ont lancé le Programme pilote d'apostilles électroniques (e-APP). Dans le cadre de ce programme, la Conférence de La Haye et l'Association nationale des notaires des États-Unis s'emploient, avec tout État intéressé, à mettre au point, promouvoir et faciliter l'application de logiciels pour: *a)* la délivrance et l'utilisation d'apostilles électroniques et *b)* le fonctionnement de registres électroniques d'apostilles[147]. Le Programme envisage deux formats distincts mais finalement identiques d'apostilles électroniques. Les deux méthodes protègent le document sous-jacent et le certificat d'apostille électronique contre les modifications non autorisées, mais chacune offre une interface différente au destinataire.

114. En vertu de la première méthode, une autorité compétente peut ajouter le certificat d'apostille en dernière page d'un acte public sous-jacent, existant dans un format donné (le Programme pilote d'apostilles électroniques s'intéresse aux documents échangés dans le format PDF, Portable Document Format). Le destinataire ouvre le document et trouve le certificat d'apostille électronique intégré en dernière page du même document. Si ce format est choisi, le document public sous-jacent et le certificat d'apostille électronique constituent un document unique et continu, ou en d'autres termes, un fichier unique. On peut toujours décider d'imprimer une ou plusieurs pages de ce fichier unique, de sorte que le certificat d'apostille électronique pourrait être imprimé seul[148].

115. En vertu de la seconde méthode, le document public sous-jacent est joint au certificat d'apostille électronique à titre de fichier distinct. Le destinataire reçoit un fichier PDF unique mais, à l'ouverture du fichier, l'utilisateur visionne d'abord le certificat d'apostille électronique et peut alors ouvrir le document public sous-jacent joint afin de le visionner comme un fichier PDF distinct. L'avis a été émis que cette méthode offrirait une interface plus intuitive au destinataire du document revêtu de l'apostille (par exemple, le Département d'État des États-Unis l'a adoptée pour ses dépôts de brevets électroniques et comme modèle pour l'apostille électronique). En joignant

[145]Conférence de La Haye de droit international privé, "Conclusions et recommandations adoptées par la commission spéciale…".

[146]Conférence de La Haye de droit international privé "Conclusions et recommandations adoptées par la commission spéciale…", paragraphe 24.

[147]Christophe Bernasconi et Rich Hansberger, "Electronic Apostille Pilot Program (e-APP): memorandum on some of the technical aspects underlying the suggested model for the issuance of electronic apostilles (e-apostilles)" (accessible sur le site Internet: http://www.hcch.net/upload/wop/genaff_pd18e2007.pdf (consulté le 26 mai 2008).

[148]"Programme pilote d'apostilles électroniques…", paragraphe 18.

l'acte public sous-jacent, sous forme de fichier, au certificat d'apostille électronique, on vise très clairement à informer le ou la destinataire, lors de sa première ouverture du document, qu'il s'agit d'une apostille. À partir de là, il ou elle peut ensuite ouvrir l'acte public sous-jacent afin d'en visionner le contenu"[149].

116. Quel que soit le modèle retenu, le fonctionnement des apostilles électroniques entraîne la délivrance de certificats sous forme électronique, porteurs d'une signature numérique apposée par l'autorité compétente voulue, aux fins de la convention Apostille de La Haye. Chaque autorité compétente conservera en outre un registre sous forme électronique autorisant une vérification des certificats délivrés à l'appui des apostilles électroniques[150].

117. Dans les pays qui ont aboli les lois ou les exigences afférentes aux apostilles, on peut imaginer d'élaborer des systèmes grâce auxquels les enregistrements notariés étrangers acquerraient une reconnaissance juridique fondée sur la vérification de la signature électronique ou une méthode d'authentification utilisée par le notaire émetteur. La signature électronique du notaire émetteur doit être vérifiable par l'utilisateur du document (généralement un autre notaire) de façon simple et rapide. Ceci peut être effectué via l'Internet en accédant au site du prestataire de services de certification du notaire émetteur qui, en Europe au moins, est généralement la chambre nationale dont est membre ce notaire. Parallèlement, il convient d'examiner la question de la vérification du pouvoir du notaire d'origine d'authentifier des enregistrements en vertu du système juridique dans le cadre duquel il ou elle travaille. Afin de faciliter ce processus et de parer au besoin de consulter un éventuel organe de supervision étranger validé par les notaires émetteurs de licences, il a été proposé que les prestataires de services de certification établis sous les auspices des chambres notariales n'émettent des certificats qu'aux notaires autorisés au moment pertinent à exercer cette fonction, de sorte que toute suspension ou révocation d'un pouvoir notarial empêche automatiquement la vérification de la signature du notaire concerné[151].

b) Applications nationales: sceaux, notarisation et attestation

118. Quelques pays ont déjà éliminé l'exigence du sceau, l'apposition d'un sceau n'apparaissant plus comme pertinente dans le contexte contemporain. Une signature attestée (c'est-à-dire donnée en présence d'un témoin) l'a remplacée[152]. Les législations d'autres pays considèrent que des signatures électroniques sécurisées répondent aux exigences du sceau. L'Irlande, par exemple, a promulgué des dispositions spécifiques

[149]"Programme pilote d'apostilles électroniques…", paragraphe 19.

[150]Pour de plus amples informations sur le fonctionnement des apostilles électroniques, voir le site Internet du Programme pilote d'apostilles électroniques: http://www.e-app.info/ (consulté le 6 juin 2008).

[151]Ugo Bechini et Bernard Reynis, "La signature électronique transfrontière des notaires: une réalité européenne", *La semaine juridique (édition notariale et immobilière),* n° 39 (24 septembre 2004), page 1447 .

[152]Au Royaume-Uni, par exemple, la loi sur la propriété (*Law of Property* (Miscellaneous Provisions) *Act)* de 1989, qui a mis en œuvre le Rapport de la Commission de réforme des lois sur les actes et actes en tierce ("Deeds and Escrows") (Law Com. No.143, 1987).

concernant les signatures électroniques sécurisées selon lesquelles celles-ci peuvent, si elles sont certifiées comme il convient, être utilisées en lieu et place d'un sceau, sous réserve de l'assentiment de la personne ou de l'organisme public auquel peut ou doit être remis le document revêtu d'un sceau[153]. Au Canada, l'exigence que la signature d'une personne soit accompagnée d'un sceau prévu par certaines lois fédérales se trouve satisfaite par une signature électronique sécurisée identifiant celle-ci comme étant le sceau de l'intéressé[154].

119. Un certain nombre de pays ont lancé des initiatives envisageant l'utilisation de documents et de signatures électroniques dans le cadre des transactions faisant intervenir des titres de propriété immobilière. Le modèle utilisé dans l'État de Victoria, en Australie, envisage l'utilisation d'une technologie de signatures numériques sécurisées via l'Internet au moyen de cartes numériques délivrées par une autorité de certification. Au Royaume-Uni, le modèle prévoit qu'un avocat pourra signer un titre de propriété immobilière au nom de son client via un intranet. Dans certains pays, la possibilité d'utiliser des "sceaux électroniques", par opposition à des sceaux manuels est officiellement reconnue, tandis que le soin de déterminer séparément les détails techniques relatifs à la forme que doit revêtir le sceau électronique est laissé à d'autres instances[155].

120. Aux États-Unis, la Loi uniforme sur l'enregistrement électronique des biens immobiliers[156] stipule expressément qu'une signature électronique n'a pas à être accompagnée d'un timbre, d'une impression ou d'un sceau, sous leur forme physique électronique. Ce n'est, au fond, que l'information figurant sur le sceau, plutôt que celui-ci, qui est requise. Elle prévoit aussi qu'une signature électronique répond à toute loi, tout règlement ou toute norme exigeant un timbre, une impression ou un sceau personnel ou social. Ces indices physiques ne sont pas applicables à un document totalement électronique. Cependant, cette loi stipule que les informations qui figureraient autrement sur le timbre, l'impression ou le sceau doivent être jointes au document ou à la signature électronique ou y être logiquement associées par la voie

---

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

[154]Canada, article 39 de la Partie 2 de la Loi sur la protection des renseignements personnels et les documents électroniques. Les lois fédérales en question sont la Loi sur les Immeubles fédéraux et les biens réels fédéraux et le Règlement concernant les immeubles fédéraux.

[155]On peut en citer à titre d'illustration les règles relatives à la validation de documents par des professionnels agréés ou accrédités, par exemple la Loi sur les ingénieurs et les géoscientifiques (Manitoba, Canada) eu égard à l'Association des ingénieurs et des géoscientifiques du Manitoba, qui définit un "sceau électronique" comme étant la forme d'identification délivrée par l'Association à tout membre aux fins de son utilisation dans la validation électronique de documents sous forme lisible par ordinateur (voir: http://apegm.mb.ca/keydocs/act/index.html consulté le 6 juin 2008).

[156]La Loi uniforme sur l'enregistrement électronique des biens immobiliers (*Uniform Real Property Electronic Recording Act*) des États-Unis a été rédigée par la National Conference of Commissioners on Uniform State Laws, et est accessible sur le site Internet à l'adresse http://www.law.upenn.edu/bll/ulc/urpera/URPERA_Final_Apr05-1.htm (consulté le 6 juin 2008). La Loi uniforme a été adoptée par les États suivants: Arizona, Arkansas, Caroline du Nord, Caroline du Sud, Connecticut, Delaware, District de Columbia, Floride, Idaho, Illinois, Kansas, Minnesota, Nevada, Nouveau Mexique, Tennessee, Texas, Virginie, Washington et Wisconsin (voir: http://www.nccusl.org, consulté le 20 mars 2008).

électronique[157]. Ainsi, conformément à cette loi, le timbre ou le sceau notarial qu'exige la législation de certains États n'est pas nécessaire, pour une notarisation électronique. Le timbre ou le sceau de la société qui doit être apposé conformément à la législation de certains États pour authentifier l'acte d'un fondé de pouvoir d'une société n'est pas nécessaire non plus.

121. Les sceaux ne sont pas d'usage fréquent sur les documents privés établis dans les pays de droit romain, mais la plupart de ces pays ont très largement recours à la notarisation pour garantir l'identité des personnes et l'authenticité des documents. Dans plusieurs, les notaires ont déjà fait des technologies de l'information et des télécommunications un outil normatif de leur travail. Dans beaucoup, les chambres notariales ont mis sur pied des prestataires de services de certification chargés de délivrer des certificats validant l'utilisation des signatures électroniques (habituellement des signatures numérisées) par les notaires membres de leur organisation, et parfois aussi par le public.

122. En Italie, le 12 septembre 2002, l'Autorité chargée des technologies de l'information dans l'administration publique a autorisé le Conseil national du notariat à offrir des services de certification aux notaires italiens, dont les signatures numérisées peuvent être vérifiées en ligne[158]. En outre, les notaires italiens procèdent actuellement à une migration complète vers les technologies informatiques pour la transmission des enregistrements auprès des registres publics. Par exemple, pour la transmission aux registres commerciaux des actes constitutifs et des statuts de sociétés, ou de leurs amendements, les documents papier ont d'ores et déjà été totalement éliminés. Des progrès significatifs ont également été réalisés pour la transmission électronique des enregistrements de transactions relatives aux biens immobiliers, même si les documents papier sont encore en usage en raison, est-il expliqué, de retards dans l'introduction des technologies de communication informatique dans les rouages judiciaires. Ces services sont fournis avec l'aide d'une société spécialement créée en 1997 par le Conseil national du notariat et la Caisse nationale du notariat dans le but de gérer les services relatifs aux technologies de l'information et de la communication, pour les notaires italiens[159]. Un système semblable est utilisé en Espagne, où le Conseil général du notariat a créé sa propre autorité de certification, et où les notaires ont mis sur pied un système de dépôt électronique des enregistrements auprès des registres de commerce[160].

123. En France, le texte révisé de l'article 1317 du code civil permet, par exemple, l'enregistrement d'actes authentiques sur support électronique dans des conditions fixées par décret en Conseil d'État. Le Conseil supérieur du notariat a mis en place un système de certification des signatures numérique auquel les notaires français ont recours[161]. Ce système est certifié par une société créée par plusieurs organismes de

[157] C'est-à-dire des critères semblables à ceux prévus par la Loi uniforme relative aux transactions électroniques des États-Unis.

[158] Voir: http://ca.notariato.it (consulté le 6 juin 2008).

[159] Voir: www.notariato.it, sous "Servizi Notartel" (consulté le 6 juin 2008)

[160] Voir: http://www.notariado.org/n_tecno/ (consulté le 6 juin 2008).

[161] "La signature électronique notariale certifiée", *La revue fiscale notariale*, n° 10 (octobre 2007), Alerte 53.

l'État pour offrir des services de certification. Bien que les notaires français n'utilisent pas encore la transmission électronique des actes aussi intensément que leurs homologues italiens ou espagnols le développement de l'application Télé@actes, en mai 2006, devrait leur permettre d'échanger des titres de propriété avec la conservation des hypothèques, sous une forme entièrement électronique. La numérisation des titres de propriété immobilière sera aussi bientôt possible.

124. En Allemagne, la loi fédérale d'accélération des procédures d'enregistrement, de 1993[162] a permis d'informatiser les enregistrements obligatoires d'actes relatifs aux transactions immobilières, commerciales et autres. Les administrations judiciaires non centrales ont utilisé cette possibilité à plus ou moins grande échelle et en faisant appel à des approches techniques diverses[163]. L'introduction d'un système de registre électronique a permis aux notaires allemands d'échanger des informations directement avec les registres au moyen des communications électroniques. Afin de s'assurer que les enregistrements notariés électroniques offrent le même degré de fiabilité que les enregistrements papier, les notaires allemands ont mis sur pied un prestataire de service de certification respectant la loi allemande sur les signatures électroniques. Ce prestataire a été agréé par l'organe de réglementation des télécommunications allemandes le 15 décembre 2000. À l'instar d'autres pays, les notaires allemands ont mis en place un système de certification fondé sur une infrastructure à clef publique utilisant la technologie de la signature numérique. Les certificats délivrés par le prestataire de services de certification de la Chambre fédérale des notaires certifient non seulement la clef publique utilisée par le notaire pour signer les documents, mais aussi le pouvoir du signataire en tant que notaire agréé. Dans le système allemand, les signatures numériques servent à authentifier des enregistrements au moment de leur création et lors de toute reproduction. Les lignes directrices publiées par la Chambre fédérale allemande des notaires rappellent à ces derniers la nécessité de veiller à la sûreté de la transmission des documents électroniques, par exemple en utilisant uniquement des connexions sécurisées SSL[164]. Pour faciliter le traitement des enregistrements électroniques par les registres, ou bien leur utilisation par les usagers, les notaires allemands sont tenus de créer les documents dans un format normalisé (XML ou Extensible Markup Language)[165]. Les règles allemandes d'émission des enregistrements électroniques exigent deux niveaux d'authentification par le notaire. Tous les enregistrements électroniques, ainsi que leurs annexes et les fichiers contenant la signature numérique du notaire sont liés et archivés ensemble en format de fichiers ZIP et le fichier ZIP entier lui-même est authentifié une fois encore avec la signature numérique du notaire.

---

[162] Allemagne, Bundesgesetztblatt, Part I, 20 décembre 1993, page 2182).

[163] Voir les informations sur l'ampleur de la mise en œuvre des registres électroniques en Allemagne par la Chambre fédérale des notaires de ce pays (http://www.bnotk.de/Service/Elektronischer_Rechtsverkehr/Registerelektronisierung.html (consulté le 6 juin 2008)).

[164] Voir *"Empfehlungen zur sicheren Nutzung des Internet"*, Rundschreiben Nr. 13/2004 der Bundesnotarkammer vom 12.03.2004 (accessible sur le site Internet: http://www.bnotk.de/Service/Rundschreiben/RS.2004.13.sichere.Internetnutzung.html, consulté le 6 juin 2008).

[165] Voir *"Hinweise und Anwendungsempfehlungen für den elektronischen Handels-, Genossenschafts- und Partnerschaftsregisterverkehr*" Rundschreiben 25/2006 der Bundesnotarkammer vom 07.12.2006 (accessible sur le site Internet: http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html (consulté le 6 juin 2008)).

125. Les équivalents électroniques des actes notariés sont également de plus en plus utilisés en Autriche. Les éléments essentiels du système autrichien de notarisation électronique sont d'une façon générale similaires à ceux du système allemand. Le système autrichien présente néanmoins un trait original, à savoir l'établissement d'un registre électronique centralisé ("cyberDOC") destiné à une conservation sécurisée des documents sous forme électronique. Une société indépendante créée conjointement par la Chambre autrichienne du notariat de droit civil et Siemens AG, met à la disposition des notaires un système d'archivage électronique qui comporte des fonctions d'authentification[166]. Les notaires autrichiens sont tenus par la loi d'y verser tous les actes notariaux établis après le 1er janvier 2000.

126. Même si de manière générale la fonction d'authentification du notaire eu égard aux signatures peut être reproduite dans un environnement électronique par l'utilisation de méthodes d'authentification et de signature électroniques, d'autres fonctions réclament des solutions plus larges. Un trait caractéristique des actes notariés est qu'ils doivent mentionner, selon le cas, la date à laquelle ils sont établis, la date à laquelle ils sont enregistrés, la date à laquelle ils sont signés ou copiés. Il a été remarqué qu'un usage simple de techniques automatiques pourrait se substituer à l'apposition d'une date certifiée par un notaire[167].

127. Plus importantes cependant sont les procédures de tenue à jour des registres électroniques des actes notariés. La loi impose généralement aux notaires d'archiver l'enregistrement des documents qu'ils reçoivent ou produisent. Copier cet enregistrement général dans un environnement électronique comporte un certain nombre de difficultés. Un autre problème – plus grave encore – concerne le risque d'incompatibilité technique entre différents logiciels et équipements susceptibles d'être utilisés par les notaires à cette fin. L'évolution rapide des technologies de l'information et des technologies de communication augmente le besoin migration des données d'un format ou support vers un autre. La possibilité de lire les données migrées sur de nouveaux formats ou supports n'est cependant pas toujours garantie. Il est donc nécessaire de concevoir des procédures de contrôle permettant de vérifier l'intégrité des contenus d'un enregistrement, préalablement à la migration et après celle-ci. Ainsi qu'il a déjà été remarqué, la technologie de chiffrement fondée sur les infrastructures à clef publique ne garantit pas nécessairement la possibilité de lire les signatures numériques elles-mêmes dans la durée (voir paragraphe 51 ci-dessus). Il faudra donc veiller à une gestion soigneuse du processus de migration, et éventuellement confirmer l'authentification utilisée originellement. Il a été établi que, pour assurer la cohérence et l'interopérabilité, il est préférable de charger un tiers de confiance de cette fonction, plutôt que de la confier à chaque notaire[168].

128. C'est, par exemple, le modèle que le législateur a finalement retenu en France. La récente réforme des règles régissant les actes établis par les notaires a posé les

[166]Voir Österreichische Notariatskammer (Chambre autrichienne du notariat de droit civil), accessible sur le site Internet: http://www.notar.at, sous "Cyberdoc" (consulté le 6 juin 2008).

[167]Didier Froger, "Les contraintes du formalisme et de l'archivage de l'acte notarié établi sur support dématérialisé", *La semaine juridique (édition notariale et immobilière)*, n° 11 (12 mars 2004), page 1130.

[168]Didier Froger, "Les contraintes du formalisme…".

conditions générales d'équivalence fonctionnelle entre les actes notariés sur papier et les enregistrements électroniques[169]. Entre autres dispositions concernant principalement la sécurité des informations, les nouvelles règles ont instauré un minutier central des actes notariés sur support électronique qui garantit que les actes notariés: sont conservés dans des conditions de nature à en préserver l'intégrité; restent accessibles exclusivement aux notaires qui les ont établis; puissent subir des opérations de migration vers de nouveaux formats en raison des besoins techniques sans que leur contenu soit altéré; puissent se voir apposer des informations postérieures par le notaire sans qu'il en résulte une altération du contenu original.

129. Malgré les progrès réalisés ces dernières années, certains doutes subsistent quant à la manière dont les nouvelles règles autorisant les équivalents électroniques des actes notariés peuvent être conciliées avec les éléments essentiels des actes authentiques, en particulier la nécessité de la présence physique des parties devant le notaire[170]. Partant de l'hypothèse que la présence physique est indispensable à l'établissement d'un enregistrement juridiquement authentique, le défi consiste à envisager des adaptations des formes existantes aux technologies du futur[171]. À cet égard, il a été dit que la cryptologie ne se substitue pas aux symboles tangibles des autorités publiques et du consentement des parties[172]. Ainsi, certaines règles exigent que les parties et les témoins soient en mesure de voir effectivement une image de leur signature sur l'écran; de même, une image du sceau du notaire figurera dans tous les actes[173].

130. Aux États-Unis, il existe trois lois principales concernant la notarisation électronique: la Loi uniforme relative aux transactions électroniques[174], la Loi relative aux signatures électroniques dans le commerce national et international (e-sign)[175] et la Loi uniforme relative à l'enregistrement des biens immobiliers[176]. L'effet combiné desdites lois est que l'exigence légale pour qu'un document ou une signature associée à un document soit notarié, reconnu, vérifié, contresigné par un témoin ou dressé sous serment, se trouve satisfaite si la signature électronique de la personne autorisée, ainsi que toutes les autres informations devant être incluses aux termes d'autres lois applicables, sont jointes au document ou y sont logiquement associées. Un certain nombre d'États ont, depuis, mis en place des systèmes de notarisation par des moyens électroniques. Le Département d'État de Pennsylvanie, par exemple, avec une équipe spéciale de registres de comtés, a créé le Programme des registres notariés et des sceaux notariaux électroniques, qui permet une authentification des notaires en temps réel et

[169]France. Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires (*Journal Officiel*, 11 août 2005, page 96).

[170]Pierre-Yves Gautier et Xavier Linant de Bellefonds, "De l'écrit électronique et des signatures qui s'y attachent" *La semaine juridique (édition générale)*, n° 24 (14 juin 2000), I 236, paragraphes 8 à 10.

[171]Pierre Catala, "Le formalisme et les nouvelles technologies", *Répertoire du notariat Defrénois*, n° 20, 2000, pages 897 à 910.

[172]Luc Grynbaum, "Un acte authentique électronique pour les notaires", Communication Commerce électronique, n° 10, octobre 2005, com. 156.

[173]Décret n° 71-941 tel qu'amendé par le décret n° 2005-973, paragraphe 3 de l'article 17 (voir note 169).

[174]Voir note 90.

[175]Code des États-Unis, articles 7001 à 7031 du chapitre 96 du Titre 15.

[176]Voir note 156.

la délivrance en ligne sécurisée de sceaux notariés authentifiés. Ce système de notarisation électronique vise à simplifier les transactions commerciales entre les agents de l'État et le monde des affaires, ainsi qu'à accroître la protection du public contre les contrefaçons et les fraudes, tout en maintenant les composantes fondamentales de la notarisation. Le système fait usage de services de certification numériques assurés par un prestataire commercial[177].

131. Les notaires souhaitant participer à ce projet de notarisation électronique doivent faire acte de candidature auprès du Bureau des commissions, des élections et de la législation de l'État pour devenir des "notaires électroniques" agréés (*e-notary*). Le notaire doit acquitter un montant déterminé pour obtenir un certificat numérique, sous la forme d'un sceau notarial électronique, auprès de l'autorité de certification certifiée au niveau fédéral, approuvée par le Bureau de l'Administration et le Secrétaire du Commonwealth (de l'État de Pennsylvanie), et sélectionnée par les chargés d'enregistrement des actes participant au projet de notarisation électronique. Avant d'obtenir un certificat numérique, le "notaire électronique" agréé doit se rendre en personne devant l'un quelconque des chargés d'enregistrement des actes participant au projet de notarisation électronique et lui présenter une lettre d'agrément du Département d'État ainsi que des preuves satisfaisantes de son identité. Le "notaire électronique" agréé doit faire en sorte que pour chaque notarisation électronique les informations suivantes soient jointes ou logiquement associées à la signature électronique ou au document électronique à notarier, reconnaître ou vérifier: le nom complet du notaire électronique accompagné du titre "notary public," le nom de la municipalité et du comté où le notaire électronique a son étude et la date d'expiration du mandat du notaire. Le notaire doit garantir que le particulier pour lequel il ou elle agit dans le cadre d'une notarisation électronique se présente en personne devant lui ou elle pour chaque notarisation électronique réalisée. Conformément aux dispositions prises par le Département d'État de Pennsylvanie les éléments fondamentaux de la notarisation, notamment la présence en personne des signataires du document devant le notaire s'appliquent toujours. Cependant, le notaire attache numériquement ses données d'identification sur un document qui existe sous forme de données électroniques dans un format lisible par un ordinateur, plutôt que sur un document papier sur lequel il apposerait un sceau notarial en caoutchouc[178].

132. D'une manière largement similaire à ce qu'ont connu les pays de droit romain, il y a eu quelques débats dans les pays de *common law* sur la capacité des moyens électroniques à copier la fonction des méthodes traditionnelles de notarisation et d'authentification. Aussi longtemps que la notarisation se limite pour l'essentiel à confirmer l'intégrité des documents et l'identité des signataires, il ne semble pas y avoir de difficulté insurmontable dans l'usage des communications électroniques et leur équivalence avec les documents papier. Cependant, la situation devient moins claire lorsque l'authenticité d'un document ou d'un enregistrement est certifiée par une confirmation

[177] Anthony Garritano, "National e-notary standards in progress", *Mortgage Servicing News* (New York), vol. 10, n° 2, 1er mars 2006, page 11.

[178] Voir: http://www.dos.state.pa.us/dos/site/default.asp, sous "Notaries", "Electronic Notarization" (consulté le 5 juin 2008).

par un notaire de la présence d'une personne lors de l'acte de signature du document ou de l'enregistrement[179].

133. On a fait valoir que les processus classiques de vérification par un témoin, comme les attestations, qui peuvent être utilisées en relation avec, mais aussi indépendamment de, l'établissement d'un acte public par un notaire, ne se prêtent pas entièrement à la signature électronique de documents étant donné que nul ne peut avoir l'assurance que l'image apparaissant sur l'écran est en fait le document sur lequel sera apposée la signature électronique. Tout ce que peuvent voir le signataire et le témoin est une représentation à l'écran, visible à l'œil nu, de ce qui se trouve prétendument dans le système d'information. Lorsque le témoin voit le signataire taper des touches sur le clavier, il ne peut pas être certain de ce qui se passe effectivement. Il ne serait par conséquent uniquement possible d'avoir la certitude que ce qui apparaît à l'écran correspond au contenu du système d'information et que les touches utilisées par le signataire correspondent à son intention, si l'ordinateur a été validé dans sa fiabilité opérationnelle, selon des critères d'évaluation eux-mêmes fiables[180].

134. Toutefois, une signature électronique sécurisée pourrait jouer un rôle similaire à celui du témoin en identifiant la personne apparaissant comme l'auteur de la signature de l'acte. En utilisant une signature électronique sécurisée sans témoin humain, l'on pourrait vérifier l'authenticité de la signature, l'identité de la personne à laquelle appartient la signature, l'intégrité du document et probablement même la date et l'heure de la signature. En ce sens, la signature électronique sécurisée peut même être plus sûre qu'une signature manuscrite ordinaire. L'avantage de faire attester par un témoin une signature numérique sécurisée serait vraisemblablement minime, à moins que le caractère volontaire de la signature ne soit mis en question[181].

---

[179]"Avec les technologies qui permettent maintenant les "téléconférences" entre des parties se trouvant dans des villes différentes, ou même dans des pays différents, il est probable que les définitions juridiques de la "présence personnelle" s'élargiront, ce qui permettra à un notaire se trouvant à Los Angeles d'attester d'une apposition télévisée de signature par une personne se trouvant à Londres. L'interaction audio du notaire avec le signataire absent et l'acquisition en temps réel de l'image vidéo du signataire semblent être les conditions préalables à de telles notarisations électroniques à distance. Cependant, dans une situation où le notaire se trouve en un lieu et l'attestant, ou le signataire, de la déclaration sous serment se trouve en un autre lieu, ces actes notariaux électroniques sont concevables sans interaction audio, dans la mesure où l'usage généralisé du courrier électronique démontre que l'interaction visuelle semble être, elle, une condition *sine qua non*. De quelle autre façon le notaire pourrait-il déterminer que le signataire à distance n'est pas contraint de façon flagrante, et enregistrer une image visuelle constituant une preuve que l'expéditeur des données n'était pas un imposteur utilisant une clef privée volée? De la même manière que la Cour suprême du Nebraska a jugé en 1984 (*Christensen* c. *Arant*) que le simple contact auditif au travers d'une porte intermédiaire ne suffisait pas à établir la présence physique au sens juridique traditionnel du terme, il est probable que le simple contact électronique par le truchement d'un média non visuel ne suffira pas à satisfaire aux conditions d'une présence physique au sens légal du futur" (Charles N. Faerber, "Being there: the importance of physical presence to the notary," *The John Marshall Law Review*, vol. 31 (Printemps 1998), pages 749 à 776).

[180]C'est ce qui est parfois appelé le problème "*what you see is what you sign*" (WYSIWYS) (Ce que vous voyez est ce que vous signez) (voir également pour une discussion des affichages de confiance) (C. Liu *et al*., "Visually sealed and digitally signed documents", Association of Computing Machine, *ACM International Conference Proceeding Series,* vol. 56; et *Proceedings of the Twenty-seventh Australasian Conference on Computer Science,* vol. 26 (Dunedin, Nouvelle-Zélande, 2004), page 287.

[181]Voir discussions des Joint Infocomm Development Authority of Singapore and the Attorney – General's Chambers, *Joint IDA-AGC Review of Electronic Transactions Act Stage II: Exclusions under Section 4 of the ETA*, document de travail LRRD n°. 2 /2004 (Singapour, 2004), parties 5 et 8, accessible sur le site Internet: www.agc.goc.sg, sous la rubrique "Publications" (consulté le 6 juin 2008).

135. La législation existante n'est pas allée jusqu'au point de remplacer totalement les règles d'attestation par des signatures électroniques, mais permet simplement au témoin d'utiliser une signature électronique. En Nouvelle-Zélande, la Loi relative aux transactions électroniques stipule que la signature électronique d'un témoin répond aux exigences légales de la signature ou du sceau qui doit être attesté. La technologie à employer aux fins de la signature électronique n'est pas spécifiée mais doit identifier le témoin de façon adéquate et indiquer de même que la signature ou le sceau a été attesté; être aussi fiable que nécessaire étant donné le but dans lequel, et les circonstances dans lesquelles, la signature du témoin est requise[182].

136. Au Canada, la Loi sur la protection des renseignements personnels et les documents électroniques dispose que, lorsque la législation fédérale prévoit qu'une signature doit être attestée par un témoin, cette exigence est satisfaite, dans le cas d'un document électronique, si chacun des signataires et témoins appose au document électronique sa signature électronique sécurisée[183]. Dans le cas où une disposition d'un texte législatif exige une déclaration attestant la véracité, l'exactitude ou l'intégralité d'une information fournie par le déclarant, la déclaration peut être faite sous forme électronique si le déclarant y appose sa signature électronique sécurisée[184]. Dans le cas où une disposition d'un texte législatif exige une déclaration sous serment ou une affirmation solennelle, celle-ci peut être faite sous forme électronique si l'auteur appose à la déclaration ou à l'affirmation sa signature électronique sécurisée et si le commissaire aux serments devant qui a été faite la déclaration ou l'affirmation appose à celle-ci sa signature électronique sécurisée[185]. Une autre formule qui a été suggérée pour donner une assurance supplémentaire est que la signature électronique soit apposée par un professionnel fiable, comme un avocat ou un notaire, ou en sa présence[186].

---

[182]Nouvelle-Zélande, *Electronic Transactions Act* (voir la note 88, article 23)

[183]Canada, Loi sur la protection des renseignements personnels et les documents électroniques (2000°, deuxième 2, article 46.

[184]Canada, Loi sur la protection des renseignements personnels…, article 45.

[185]Canada, Loi sur la protection des renseignements personnels…, article 44.

[186]L'avocat / agent agréé immobilier (*conveyancer*) devra obtenir les signatures électroniques et l'authentification auprès d'une autorité de certification agréée. Il se peut que l'acheteur et le vendeur doivent autoriser le "*conveyancer*" à signer par procuration écrite. Voir "E-conveyancing: the strategy for the implementation of e-conveyancing in England and Wales" (Royaume-Uni, Land Registry, 2005), accessible sur le site Internet à l'adresse http://www.landregistry.goc.uk/assets/library/documents/e-conveyancing_strategy_v3.0.doc, (consulté le 5 juin 2008). Ce projet doit être mis en œuvre par étapes de 2006 à 2009.

Deuxième partie

Utilisation internationale des méthodes de signature et d'authentification électroniques

Table des matières

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

137. 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

138. 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 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.

139. 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

140. 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 (alinéa *b* du paragraphe 1 de son article 7), et la Convention des Nations Unies sur l'utilisation de communications

électroniques dans les contrats internationaux (paragraphe 3 de son article 9) font partie des instruments juridiques internationaux qui adoptent une telle approche. En vertu de cette dernière, une méthode d'authentification ou de 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.

141. 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 alors 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.

142. 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 des présomptions juridiques plus fortes 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 technologie est que ce transfert général a priori des risques juridiques peut se justifier par le niveau de fiabilité offert par une technique donnée, dès lors que 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 technologie particulière, toutes les autres – 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.

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

144. 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 posées par ces pays.

145. En second lieu, une législation technospécifique, notamment si elle favorise les signatures numériques, ce qui est également le cas de l'approche dualiste, 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[187]. En effet, un problème important non résolu relatif, notamment, aux 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) 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[188]. Pour les besoins de la présente étude, les points faibles ci-après, relevés par le Groupe de travail sur la sécurité de l'information et la vie privée de l'OCDE, peuvent présenter un intérêt:

a) Interopérabilité. On a constaté de nombreux obstacles et limites à l'interopérabilité. Au niveau technique, malgré l'abondance des normes, l'absence de normes de base communes applicables à certaines technologies a été 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, ont été considérées comme des obstacles au progrès. Selon le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée, "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 Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée, 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 Groupe de travail laisse donc entendre que c'est donc "un secteur dans lequel il serait utile de poursuivre les travaux. Étant donné que toute activité dans ce domaine est étroitement

[187]Baker et Yeo, "Background and issues concerning authentication…", idem note 93.

[188]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), (DSTI/ICCP/REG(2005)4/FINAL), accessible sur le site Internet: http://www.oecd.org/dataoecd/1/10/35809749.pdf (consulté le 6 juin 2008).

liée à la question plus générale de l'interopérabilité, ces thèmes pourraient être traités conjointement";

c) Acceptation des certificats[189]. Dans certains cas, l'acceptation des certificats délivrés par d'autres entités a été citée comme un obstacle à l'interopérabilité. Le Groupe de travail 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 juridictions sur ce thème et ils pourraient être utiles à toute initiative du Groupe dans ce domaine;

d) Une large palette de méthodes d'authentification: Le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée a constaté que dans presque tous les pays de l'OCDE, une large palette de méthodes d'authentification est déjà utilisée. Ces méthodes vont des mots de passe, d'une part, aux certificats d'authentification (*tokens*), à la signature numérique et à la biométrie, d'autre part. Selon la technologie utilisée et les contraintes correspondantes, 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 Groupe de travail, 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 Groupe de travail, 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 et/ou des utilisateurs.

146. 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 technologiquement neutre en matière de signatures et d'authentification électroniques. Toutefois, il ne serait pas réaliste d'attendre que cela rende totalement inutile l'élaboration d'une solution harmonisée pour résoudre les questions d'incompatibilité des normes techniques ou juridiques. 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 lorsqu'elles sont étrangères, et leur équivalence avec celles qu'ils utilisent, ou du moins qu'ils connaissent.

[189]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", accessible sur le site Internet: http://www.cdt.org/privacy/authentication/030513interim.shtml (consulté le 5 juin 2008).

2. Consensus émergeant

147. Les divergences entre les politiques relevées au plan international s'expliquent probablement par une combinaison de facteurs de degrés divers. Comme on l'a vu plus haut (voir paragraphes 2 à 6 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 paragraphes 83 à 112 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[190].

148. Il est également possible que les différentes politiques reflètent différentes hypothèses quant à l'évolution des techniques d'authentification. Un scénario, dit "paradigme d'authentification universelle"[191], 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, indépendamment de tout 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, dit du "paradigme d'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[192]. 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, et soumises à des conditions communes d'utilisation de cette technologie. Dans à ce modèle, l'accent est mis sur la reconnaissance juridique des accords contractuels.

149. Malgré ces divergences, qui subsistent en partie, les conclusions du Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée[193] laissent penser 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:

---

[190]Baker et Yeo, "Background and issues concerning authentication…".

[191]Baker et Yeo, "Background and issues concerning authentication…".

[192]Baker et Yeo, "Background and issues concerning authentication…".

[193]Organisation de coopération et de développement économiques, *L'usage transfrontalier de l'authentification dans les pays de l'OCDE...*

a) Approche non discriminatoire des signatures et des services "étrangers". Les cadres législatifs ne refusent pas 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 conditions, l'approche semble non discriminatoire, tant que les exigences locales ou des exigences équivalentes sont satisfaites. Ceci recoupe les conclusions des enquêtes précédentes réalisées par le Groupe de travail 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 était bien spécifiée. À partir de ces éléments d'information, on constate que si les cadres législatifs peuvent être technologiquement neutres, la technologie doit être spécifique lorsqu'il s'agit de décisions concernant l'administration publique;

c) Importance de l'infrastructure à clef publique (ICP). Selon le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée, 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. Elle est utilisée par des "communautés d'intérêts" spécifiques dont tous les membres semblent avoir 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.

150. De plus, le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée 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[194]).

151. Les points essentiels de ce consensus émergeant ont été rappelés dans la recommandation sur l'authentification électronique, que le Conseil de l'OCDE a adoptée le 12 juin 2007 et qui, entre autres, invite les États à:

a) Œuvrer pour l'instauration d'approches technologiquement neutres pour une authentification électronique efficace des personnes et des entités aux plans intérieurs et transfrontières;

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

b) Favoriser la mise au point, la fourniture et l'utilisation de produits et services d'authentification qui intègrent de solides pratiques commerciales, notamment des garanties techniques et non techniques répondant aux besoins des participants, s'agissant particulièrement de la sécurité et de la confidentialité de leurs informations et identités;

c) À la fois dans le secteur public et privé, encourager la compatibilité commerciale et juridique et l'interopérabilité technique des programmes d'authentification afin de faciliter les interactions et transactions transsectorielles et transjuridictionnelles en ligne, et de permettre que les produits et services d'authentification puissent être déployés aux niveaux à la fois national et international;

d) Prendre des mesures pour mieux sensibiliser tous les participants, y compris dans les économies des États non membres, aux avantages de l'utilisation de l'authentification électronique aux niveaux national et international[195].

152. Ces recommandations concordent largement avec la démarche globalement adoptée par la CNUDCI dans le domaine du commerce électronique (par exemple, facilitation plutôt que réglementation, neutralité technologique, respect de la liberté de contracter, non-discrimination). Plusieurs questions juridiques restent cependant à traiter pour faciliter l'utilisation des méthodes d'authentification et de signature électroniques aux plans internationaux et transfrontaliers.

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

153. Ainsi qu'il a précédemment été observé, l'un des principaux obstacles à l'utilisation transfrontière 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 mises en place pour promouvoir une ICP interopérable, qui servirait de fondement à des opérations sécurisées dans les applications du commerce électronique. Ces instances comprennent aussi bien des

[195]OCDE, Recommandation sur l'authentification électronique et Orientations pour l'authentification électronique, Paris, juin 2007 [accessible sur le site Internet: http://www.oecd.org/dataoecd/32/45/38921342.pdf (consulté le 6 juin 2008)].

organisations intergouvernementales[196] que des organisations mixtes publiques/privées[197] à l'échelle mondiale[198] ou régionale.

154. Certaines de ces activités techniques visent à élaborer des normes techniques en vue de fournir les informations nécessaires pour répondre à des exigences juridiques[199]. 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 exigences juridiques de forme et de fond de la reconnaissance internationale des signatures électroniques.

---

[196]Dans la région Asie-Pacifique, le forum de Coopération économique Asie-Pacifique (APEC) a fait élaborer le document "Guidelines for Schemes to Issue Certificates Capable of Being Used in Cross Jurisdiction eCommerce" (principes directeurs pour des mécanismes d'émission de certificats pouvant être utilisés dans le commerce électronique transfrontière) par son groupe spécial sur la sécurité électronique et son groupe de travail sur les télécommunications et l'information, décembre 2004) [accessible sur le site Internet: http://www.apectelwg.org/contents/documents/eSTG/PKIGuidelines-Final_2_web.pdf, (original disponible au secrétariat)]. 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 utilisés dans le commerce électronique international uniquement. 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.

[197]Au sein de l'Union européenne, l'Initiative européenne de normalisation des signatures électroniques (EESSI) a été créée en 1999 par le comité des normes pour les technologies de l'information et de communication (ICT Standards Board) afin de coordonner les activités de normalisation destinées à soutenir la mise en œuvre de la directive 1999/93/CE de l'Union européenne sur les signatures électroniques. Le comité des normes de l'ICT est une émanation du Comité européen de normalisation (CEN), lequel a été créé par des organisations nationales de normalisation et par deux organisations à but non lucratif: le Comité européen de normalisation électrotechnique (CENELEC) et l'Institut européen des normes de télécommunication (ETSI). 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), pages 211 à 242).

[198]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'infrastructure à clef publique (ICP) constitué d'utilisateurs, de vendeurs et d'experts chargés de traiter certains aspects de la mise en place de la technologie des certificats numériques. Ce comité technique sur l'infrastructure à clef publique a élaboré un plan d'action envisageant, entre autres, la définition de profils ou de principes directeurs spécifiques décrivant comment les normes devraient être utilisées dans des applications particulières pour permettre l'interopérabilité des ICP; la création de nouvelles normes si nécessaire; et la mise à disposition de tests d'interopérabilité (OASIS, comité technique sur l'ICP, plan d'action ICP de février 2004), accessible sur le site Internet: http://www.oasis-open.org/committees/pki/pkiactionplan.pdf; consulté le 6 juin 2008).

[199]L'Institut européen des normes de télécommunication (ETSI), par exemple, a élaboré une norme (TS 102 231) visant, entre autres choses, à traiter aussi la reconnaissance croisée des domaines ICP et, partant, de la validité des certificats. En résumé, la spécification technique TS 102 231 prévoit une norme pour la fourniture d'informations sur le statut des prestataires de services de certification appelé "prestataires de services de confiance" (*"trust service provider"*). Ces informations sont présentées sous la forme d'une liste signée du statut des services de confiance ("Trust Service Status List"). Cette liste établie par l'ETSI répond à l'exigence de preuves permettant d'établir 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 du statut des services de confiance doit contenir des informations permettant de déterminer si le service du prestataire de services de certification 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). La liste envisagée par la spécification technique TS 102 231 doit donc afficher 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 (consulté le 6 juin 2008)].

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

155. Le lieu d'origine est un facteur classique de 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 le pays en question agit de façon réciproque. Une autre possibilité consiste à soumettre l'effet au plan interne 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 œuvrant à l'échelle nationale. Ces approches peuvent être combinées[200].

156. 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 posées par la directive européenne sur les signatures électroniques et obtenir d'être accrédité par 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[201]. 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[202]. En cumulant, d'une part, l'exigence de l'équivalence fonctionnelle avec les normes de l'Union européenne et, d'autre part, l'obligation complémentaire

[200]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 si une autorité de certification agréée en Argentine et validée par l'organisme chargé d'appliquer la réglementation assume cette reconnaissance (voir *Ley de firma digital* (2001), art. 16).

[201]De 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".

[202]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, 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".

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[203].

157. L'article 7 de la directive européenne sur les signatures électroniques a été intégré avec quelques variantes[204]. 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 de fond

158. Fidèle à une tradition de longue date, la CNUDCI n'a pas voulu tenir compte des 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 pas tenu compte 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.

159. Le paragraphe 1 de l'article 12 de la Loi type de la CNUDCI sur les signatures électroniques 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 leurs effets. Cette détermination consistant à savoir si, ou dans quelle mesure, un certificat est susceptible de produire ses effets, 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 des États-Unis sur les signatures électroniques dans le commerce mondial et national ("United States Electronic Signatures in *Global and National Commerce Act 2000*")[205]. Ces dispositions prévoient que le lieu d'origine

[203] 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), page 58.

[204] Jos Dumortier *et al*., "The legal and market aspects of electronic signatures"…, pages 92 à 94.

[205] Code des États-Unis, article 7031 du chapitre 96 du titre 15, Principes régissant l'utilisation des signatures électroniques dans les opérations internationales).

ne doit 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[206].

160. Plutôt que de tenir compte de facteurs géographiques, la Loi type établit un critère d'équivalence de fond 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.

161. 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)[207]. 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. Un État adoptant pourrait utiliser d'autres techniques juridiques pour reconnaître a priori la fiabilité de certificats et de signatures étrangers, les déclarations unilatérales ou les traités, par exemple[208].

[206] *Loi type de la CNUDCI sur les signatures électroniques*…, deuxième partie, paragraphe 83.

[207] *Loi type de la CNUDCI sur les signatures électroniques*…, deuxième partie, paragraphe 157.

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

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

162. Ainsi qu'il a été vu ci-dessus, il ressort de l'enquête entreprise par le Groupe de travail de l'OCDE sur la sécurité de l'information et la vie privée que la plupart des cadres législatifs étaient, au moins en principe, non discriminatoires à l'égard des méthodes de signature et d'authentification électroniques étrangères, dans la mesure où celle-ci répondaient aux normes locales ou à leur équivalent, en ce sens qu'ils ne refusaient pas de reconnaître l'effet juridique des 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[209]. Cependant, ce même Groupe de travail a également relevé que les mécanismes de reconnaissance des services d'authentification étrangers n'étaient généralement pas suffisamment 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 Groupe de travail a été d'avis que les deux thèmes pourraient être combinés. Il a suggéré de rédiger un document de bonnes pratiques ou des lignes directrices. Plus récemment, l'OCDE a observé que des mécanismes de reconnaissance des services d'authentification étrangers ont été mis sur pied, mais que l'on a peu d'expérience des applications transjuridictionnelles. De plus, il manque aux juridictions des moyens d'évaluer le cadre régissant la confiance chez leurs partenaires. Bien que l'OCDE ait exprimé l'espoir que ses propres lignes directrices et le cadre qu'elles offrent puissant apporter une aide à cet égard, elle a souligné que des travaux plus complets sur cette question étaient nécessaires[210]. Les sections ci-après traitent 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 s'intéressent principalement aux questions découlant de l'utilisation internationale de méthodes de signature et d'authentification électroniques étayées par des certificats délivrés par un prestataire de services de certification de confiance, et en particulier des signatures numériques créées dans le cadre d'une infrastructure à clef publique, 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 la participation de tiers dans le processus de signature ou d'authentification.

---

[209]Organisation pour la coopération et le développement économiques, *L'usage transfrontalier de l'authentification dans les pays de l'OCDE*.

[210]OCDE, Recommandation sur l'authentification électronique, page 27.

A. Types et mécanismes de reconnaissance croisée

163. 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[211]. Par exemple, les lois qui réglementent les moyens par lesquels les autorités nationales reconnaissent les signatures électroniques et certificats étrangers risquent de constituer une discrimination à l'égard des entreprises étrangères. À ce jour, tous les législateurs qui ont réfléchi à 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 étranger, 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 restrictions géographiques ou procédurales qui empêchent la reconnaissance transfrontière des signatures électroniques.

164. En l'absence d'infrastructures à clef publique 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 dite de "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 mutuellement les services qu'elles fournissent, de sorte que leurs usagers respectifs 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 lorsque de multiples politiques de sécurité interviennent, au moment, par exemple, de déterminer la partie dont la faute a causé un préjudice, et sur quelles déclarations l'usager a fait fond.

1. Reconnaissance croisée

165. La reconnaissance croisée est un dispositif d'interopérabilité selon lequel la partie intéressée se trouvant dans la zone couverte par une ICP peut utiliser des informations fournies par l'autorité d'une autre ICP pour procéder à une authentification dans la région de cette dernière[212]. 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

[211] 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, p. 29, accessible sur le site Internet: http://www.biac.org/statements/iccp/AGBtoWTO avril1999.pdf (consulté le 6 juin 2008).

[212] 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 la coopération économique Asie-Pacifique, Electronic Authentication Task Group, voir *Electronic Authentication: Issues Relating to Its Selection and Use*, publication No. 202-TC-01.2 de l'APEC (APEC, 2002), accessible sur le site Internet: http://www.apec.org/apec/publications/all_publications/telecommunications.html (consulté le 6 juin 2008).

couverte par l'ICP[213]. La question de savoir s'il est possible de se fier à une zone d'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.

166. La reconnaissance croisée intervient habituellement au niveau de l'ICP plutôt qu'à celui du prestataire de services de certification. Ainsi, lorsqu'une ICP donnée en reconnaît une autre ICP, elle reconnaît automatiquement tous les prestataires de services de certification agréés par cette dernière. La reconnaissance est fondée sur une évaluation du processus d'agrément de l'autre ICP plutôt que sur une analyse de chaque prestataire 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 en vue de leur utilisation dans les deux régions, sur la base d'une évaluation de cette catégorie de certificats.

167. 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 accéder 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 ils 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 "bas niveau" ou 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 202 à 210). Il convient par conséquent d'établir l'équivalence entre des certificats fonctionnellement comparables.

168. 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[214], ni les affirmations faites au sujet des pratiques d'établissement des certificats[215], dans la mesure où c'est la partie intéressée qui détermine si elle acceptera le certificat étranger après s'être attachée 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

[213]Définition fondée sur les travaux du Groupe de travail de l'APEC sur les télécommunications et l'information, Groupe spécial sur l'authentification électronique.

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

[215]Les affirmations en question sont une déclaration d'un prestataire de services de certification concernant les pratiques qu'il suit lorsqu'il établit un certificat.

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 clef publique

169. Par certification croisée, l'on entend la pratique consistant à reconnaître la clef 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.

170. Une certification croisée suppose l'interopérabilité technique et l'harmonisation des politiques et pratiques relatives à l'établissement des certificats. Cette harmonisation est indispensable pour faire en sorte que les domaines ICP soient compatibles pour ce qui est de leurs opérations de gestion des certificats (c'est-à-dire délivrance, suspension et révocation des certificats) aussi bien que de leur respect des normes opérationnelles et des règles de sécurité similaires. L'étendue de la couverture de 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.

171. 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 les courriels ou les applications financières. Elle peut se trouver considérablement facilitée par l'existence de systèmes techniquement compatibles, de politiques convergentes et de structures juridiques identiques.

172. La certification croisée unilatérale (un domaine ICP se fiant à un autre mais sans contrepartie) 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 où 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

173. 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[216]. Du point de vue juridique, il faut pour cela évaluer l'équivalence entre trois éléments principaux: équivalence de valeur juridique; équivalence des obligations juridiques; et équivalence de responsabilité.

174. L'équivalence de valeur juridique signifie qu'il est attribué à une signature et à un certificat étranger 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, paragraphes 107 à 112). Pour reconnaître l'équivalence des obligations juridiques et des régimes de responsabilité, il faut pouvoir déterminer que les obligations imposées aux parties qui opèrent dans le cadre d'un régime d'ICP correspondent essentiellement à celles que prévoit le régime national et que la responsabilité en cas de violation desdites obligations est essentiellement la même.

175. Dans le contexte des signatures électroniques, la responsabilité 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 un tiers spécialisé, 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 le tiers qui se fie à la signature. Dans la mesure où les actes ou omissions d'une partie causent un préjudice à l'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 de responsabilité. La loi peut demeurer muette sur ce point. Aux États-Unis, la loi de 2000 relative aux signatures électroniques dans le commerce national et international[217] 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[218];

---

[216]Aux États-Unis, par exemple, le Groupe de travail sur les politiques en matière de certification (Certificate Policy Working Group) du Bureau fédéral chargé de la politique des infrastructures à clef publique (Federal Public Key Infrastructure Policy Authority) a mis au point une méthodologie visant à porter une appréciation sur l'équivalence entre des éléments de politiques applicables (sur la base de cadres/questionnaires 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 6 juin 2008)].

[217]Code des États-Unis, article 7031 du chapitre 96 du titre 15.

[218]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 dans les contrats, ainsi que les restrictions 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), pages 43 à 47), accessible sur le site Internet: http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf (consulté le 6 juin 2008)).

b) Normes de conduite et règles de responsabilité applicables uniquement aux prestataires de services de certification. Une autre approche est celle qui consiste à ce que la loi ne réglemente 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 sur un cadre communautaire pour les signatures électroniques[219], dont le vingt-deuxième alinéa du préambule stipule que "les prestataires de service de certification fournissant des services de certification au public sont soumis à la législation nationale en matière de 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, désigne des signatures numériques basées sur ICP exclusivement[220];

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 pour 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, qui définit les normes de conduite du signataire (article 8), du prestataire de services de certification (article 9) et de la partie se fiant à la signature ou au 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.

176. Les différences entre les régimes nationaux de responsabilité peuvent constituer un obstacle à la reconnaissance transfrontière des signatures électroniques. Il y a deux raisons essentielles à cela. Premièrement, il se peut que les prestataires de services de certification hésitent à reconnaître les certificats étrangers ou les clefs 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 restrictions 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 de méthodes de signature et d'authentification électroniques ou les activités des prestataires de services de

[219] *Journal officiel des Communautés européennes*, L 13/12], 19 janvier 2000.

[220] 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 l'article 4 du Décret de 2002 relatif aux signatures électroniques du Royaume-Uni.

certification, elle subordonne habituellement leur reconnaissance des certificats ou l'agrément des prestataires de services de certification étrangers à une évaluation des équivalences de fond avec la fiabilité offerte par les certificats et les prestataires de services nationaux. Les normes de diligence et les divers niveaux de responsabilité auxquels sont soumises les 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 non plus d'avoir un impact sur le niveau d'équivalence reconnu à ses certificats.

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

177. L'attribution 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 le 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[221]. Dans la plupart des systèmes juridiques, le fondement de la responsabilité (qu'elle soit contractuelle ou quasi-délictuelle) aura des conséquences larges et significatives pour le régime de responsabilité, en particulier en ce qui concerne les éléments suivants: *a)* le degré de faute requis pour engager la responsabilité d'une partie (autrement dit, quelle est le "degré de diligence" dû à une partie par l'autre); *b)* les parties qui peuvent réclamer des dommages-intérêts 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 rejeter sa responsabilité, et dans quelle mesure.

178. 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 pays donné, 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, fondée sur la *common law* ou 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 envisagées par les législations nationales.

---

[221] Steffen Hindelang discute en détail de la possibilité, en droit anglais, de créer une relation contractuelle entre le prestataire de services de certification et la tierce partie, et parvient à une conclusion négative ("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*, No. 1, 2002, accessible sur le site Internet: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/hindelang (consulté le 6 juin 2008). Il y a néanmoins des pays où une relation contractuelle pourrait prendre naissance.

a) Degré de diligence

179. 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[222].

i) *Négligence ordinaire*

180. 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, le degré de diligence généralement requis est une "diligence raisonnable", laquelle doit être définie simplement comme le degré de diligence qu'une personne faisant montre d'une prudence, connaissance et capacité de prévoyance ordinaires exercerait dans des circonstances semblables. Dans les pays de *common law*, l'on évoque souvent le comportement d'une "personne raisonnable" tandis que les pays de droit romain se réfèrent à la notion 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 ou de projet 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 de l'autre partie à ses obligations.

181. La diligence raisonnable (ou la négligence ordinaire) est le degré général de diligence exigé par la Loi type de la CNUDCI sur les signatures électroniques. Ce degré 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[223]. On peut avoir recours à plusieurs facteurs pour évaluer la mesure dans laquelle le prestataire de services de certification respecte ce degré général de diligence[224]. La même norme

[222]Pour une discussion du système de responsabilité dans ce contexte, voir Balboni, "Liability of certification service providers …", pages 232 et suivantes.

[223]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 des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou figurant dans le certificat sont exactes et complètes; *c)* fournit à toute partie se fiant au certificat des moyens raisonnablement accessibles de déterminer à partir de ce certificat: […]; *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: […]".

[224]*Loi type sur les signatures électroniques*… 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".

s'applique également aux signataires, qui doivent empêcher toute utilisation non autorisée et conserver en sécurité leurs dispositifs de création des signatures[225]. La Loi type étend la même norme générale de diligence raisonnable à la partie qui se fie au certificat, laquelle est censée prendre 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 limite concernant celui-ci[226].

182. Quelques pays, habituellement des pays ayant incorporé à leur droit interne la Loi type de la CNUDCI sur le commerce électronique, ont adopté la norme générale de "diligence raisonnable" pour définir les normes de conduite applicables au prestataire de services de certification[227]. Dans quelques pays, il apparaît que le prestataire de services de certification "sera le plus probablement tenu par une norme générale de diligence raisonnable", même si le fait que les prestataires de services de certification sont, par nature, des parties dotées de compétences spécialisées en lesquelles les profanes placeront une confiance allant au-delà de celle qu'ils accordent aux acteurs qui interviennent normalement sur les marchés "pourrait éventuellement déboucher sur l'acquisition d'un statut professionnel ou, de quelque autre manière, les soumettre à une obligation de diligence plus élevée, les contraignant à faire ce qui est raisonnable compte tenu de leurs compétences spécialisées"[228]. En fait, comme indiqué ci-dessous (voir paragraphe 189), telle paraît être la situation dans la plupart des pays.

183. 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[229]. 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[230]. Dans

---

[225]L'article 8 de la Loi type se lit en partie énonce: "Lorsque des données afférentes à la création de signature peuvent être utilisées pour créer une 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 pour aviser toute personne dont il peut raisonnablement penser qu'elle se 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". De plus, le signataire doit prendre "des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes".

[226]Paragraphe *a)* et alinéas i et ii du paragraphe *b)* de l'article 11.

[227]Par exemple, Îles Caïmanes, article 28 de la loi de 2000 relative aux transactions électroniques et Thaïlande, article 28 de la loi de 2000 sur les transactions électroniques.

[228]"Certification authority: liability issues", étude établie pour l'American Bankers Association par Thomas J. Smedinghoff, février 1998, section 1.1, accessible sur le site Internet: http://www.wildman.com/resources/articles-pdf/ca-liability-analysis.pdf (consulté le 6 juin 2008).

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

[230]Par exemple, Argentine, *Ley de firma digital (2001)*, article 25; Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 17; Îles Caïmanes, *Electronic Transactions Act, 2000*, article 31; Inde, *Information Technology Act, 2000*, articles 40 à 42; Maurice, *Electronic Transactions Act 2000*, articles 33 à 36; Pérou, *Ley de firmas y certificados digitales*, article 17; Turquie, Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la loi de 2005 relative aux signatures électroniques, article 15; Tunisie, Loi relative aux échanges et au commerce électroniques, article 21; et Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

certains pays, cependant, la loi complète expressément la liste d'obligations par une règle générale de responsabilité du ou de la signataire en cas de violation de ses obligations[231], responsabilité qui peut même, dans un cas, avoir un caractère pénal[232]. 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 avancées[233].

184. 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 prévoient rarement plus qu'une liste générale d'obligations essentielles lorsqu'elles traitent du rôle des parties qui se fient aux certificats. Tel est généralement le cas dans les pays qui ont adopté la Loi type de la CNUDCI sur les signatures électroniques, qui recommande une norme de diligence raisonnable en ce qui concerne la conduite de la partie qui se fie au certificat[234]. Dans certains, cas cependant, cette règle n'est pas prévue expressément[235]. 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 la part de celle-ci à son obligation de diligence peut permettre au prestataire de services de certification de se défendre 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.

---

[231]Chine, Loi relative aux signatures électroniques, promulguée en 2004, article 27; Colombie, *Ley 527 sobre comercio electrónico*, article 40; Fédération de Russie, Loi fédérale sur les signatures électroniques numériques (2002), clause 12; Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99; Panama, *Ley de firma digital (2001)*, articles 37 et 39; République Dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, articles 53 et 55; Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas*, article 19; Viet Nam, Loi relative aux signatures électroniques, article 25.

[232]Pakistan, *Electronic Transactions Ordinance, 2002*, article 34.

[233]Par exemple, *Singapour Electronic Transactions Act*, chapitre 88. 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 clef privée correspondant à la clef publique indiquée dans le certificat; *b)* toutes les affirmations du 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 clef privée correspondant à la clef 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 Venezuela (République bolivarienne du) , où l'article 19 de la *Ley sobre mensajes de datos y firmas electrónicas* qualifie expressément de "diligence nécessaire" l'obligation d'éviter toute utilisation non autorisée du dispositif, tandis que d'autres obligations sont exprimées en termes stricts.

[234]Îles Caïmanes, *Electronic Transactions Act, 2000*, section 21; Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 107; et Thaïlande, Loi relative aux transactions électroniques (2001), article 30.

[235]Turquie, Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la loi de 2005 relative aux signatures électroniques, article 16; Viet Nam, Loi relative aux transactions électroniques, article 26.

ii) *Présomption de négligence*

185. 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.

186. En droit civil, il peut y avoir présomption de faute en cas de violation du contrat[236], ainsi que dans divers cas de responsabilité quasi-délictuelle. L'on peut en citer comme exemples la responsabilité indirecte 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.

187. 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[237]. Cela ne signifie pas nécessairement que la charge de la preuve 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 de *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[238].

188. Si cette règle est appliquée aux activités des prestataires de services de certification, alors, dans tous les cas où une partie qui se fie à un certificat, ou bien un

---

[236]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. 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. 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*, n° 58 à 68, août 1989).

[237]W. Page Keeton *et al*., *Prosser and Keeton on the Law of Torts*, 5e éd. (Saint Paul, Minnesota, West Publishing, 1984), section 32, page 187.

[238]"Il faut qu'une négligence soit raisonnablement établie. Lorsqu'il est démontré que la chose est sous le contrôle du défendeur ou de ses préposés et que l'accident est tel que, normalement, il n'aurait pas eu lieu si la personne ayant la garde de la chose avait fait preuve d'une diligence raisonnable, il est raisonnablement établi, en l'absence d'explication du défendeur, que l'accident est 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)].

signataire, subit un préjudice pour avoir utilisé une signature électronique ou un certificat et où 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.

189. La présomption de négligence paraît être la norme généralement applicable aux termes des législations nationales. Selon la directive de l'Union européenne sur les signatures électroniques, par exemple, le prestataire de services de certification peut voir sa responsabilité engagée à l'égard de toute entité qui fait fond raisonnablement sur le certificat qualifié, à moins que le prestataire de services n'apporte la preuve qu'il n'a pas commis de faute[239]. Autrement dit, la responsabilité du prestataire de services de certification est fondée sur la faute avec inversion de la charge de la preuve: celui-ci doit prouver que ses actes n'ont pas été négligents, étant donné que c'est lui qui est le mieux placé pour le faire, puisqu'il dispose des compétences techniques nécessaires et a accès aux informations pertinentes (que les signataires aussi bien que les tierces parties faisant fond sur le certificat risquent de ne pas avoir).

190. Tel est également le cas aux termes des droits internes de divers pays non membres de l'Union européenne, qui établissent 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[240]. Il est difficile de dire si toutes ces lois ont véritablement pour effet d'inverser la charge de la preuve, mais plusieurs d'entre elles le prévoient expressément, soit d'une manière générale[241], soit dans le contexte d'obligations spécifiques[242].

---

[239] *Journal officiel des Communautés européennes*, L 13/12, 19 janvier 2001. L'article 6 de la directive pose une norme minimale 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 désavantagerait les prestataires de services de certification établis dans un pays par rapport à ceux d'autres pays de l'Union européenne. (Balboni "Liability of certification service providers …", page 222).

[240] Argentine, *Ley de firma digital (2001)*, article 38; Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, article 31; Panama, *Ley de firma digital (2001)*, article 51; Tunisie, Loi relative aux échanges et au commerce électroniques, article 22.

[241] Chine, Loi relative aux signatures électroniques, promulguée en 2004, article 28. "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 Turquie, Loi de 2004 sur les signatures électroniques, article 13: "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".

[242] "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" (Barbade, *Electronic Transactions Act (1998)* article 20 du chapitre 308B, voir Bermudes, *Electronic Transactions Act (1999),* alinéa *b* du paragraphe 2 de l'article 23.

191. 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 constituerait 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*

192. La responsabilité objective est une règle utilisée dans divers systèmes juridiques pour attacher la responsabilité à une personne (habituellement le fabricant ou l'utilisateur de produits ou équipements potentiellement dangereux ou malsains) 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 la négligence, le manquement à une garantie ou une conduite délibérée, n'ont pas à être établis.

193. 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 par voie de conséquence 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 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[243].

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

194. 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.

[243]Par exemple, au Chili, en Équateur et au Panama.

195. D'une manière générale, la responsabilité contractuelle découle de la contravention à une obligation contractuelle. Dans un contexte d'infrastructures à clef publique (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 partie 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 d'une relation contractuelle clairement définie naîtra généralement de situations où 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 en ce qu'elle se fie aux services de certification de celui-ci. Cela peut susciter des questions difficiles qui n'ont pas toujours reçu de réponse complète dans certains pays.

196. Dans la plupart des systèmes de droit romain, 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 et donc aux informations inexactes ou fausses qu'il contenait, 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 droit romain[244], à certaines exceptions près[245]. Dans quelques pays, on peut établir une analogie entre les activités des prestataires de services de certification et celles des notaires, lesquels sont généralement tenus pour responsables du préjudice causé par toute négligence dans l'accomplissement de leurs obligations.

197. 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* exigent traditionnellement un élément de rapport contractuel 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, dans certains pays de *common law* (faute de dispositions légales expresses) la partie lésée peut rencontrer

[244]L'article 1382 du code civil français stipule que tout fait quelconque d'une personne oblige celle par la faute de laquelle il est arrivé à 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.

[245]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.

des difficultés pour établir son droit d'agir contre le prestataire de services de certification[246]. En l'absence de rapport contractuel 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"[247] 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, dès lors qu'il le fait, avec la diligence découlant d'une disposition légale, d'un contrat ou de quelque autre facteur"[248].

198. En l'occurrence, la question 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. Trois normes essentiellement peuvent être utilisées pour définir la gamme des personnes qui, en pareille situation, sont susceptibles d'intenter valablement une action contre le prestataire de services de certification[249]:

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;

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 des personnes dans l'intérêt desquelles l'on entend fournir l'information ou bien l'on sait que l'intéressé a l'intention de la fournir;

c) Norme du rapport contractuel. 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.

199. 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 se fiant

---

[246]Dans le cas de la *common law* anglaise, par exemple, un 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, on voit difficilement comment [la tierce partie] pourrait se protéger. S'il n'y a pas de responsabilité, 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), pages 149 et 150). Des conclusions similaires ont été tirées en ce qui concerne le droit australien; voir Sneddon, *Legal liability and e-transactions* …, page 15.

[247]Juge Cardozo, dans l'affaire *Ultramares Corporation* c. *George A. Touche et al*, Court of Appeals of New York, 6 janvier 1931, 174 N.E. 441, page 445.

[248]Juge Cardozo, dans l'affaire *Ultramares Corporation* c. *George A. Touche et al*… page 447.

[249]Smedinghoff, "Certification authority: liability issues", section 4.3.1.

à la signature», laquelle peut comprendre "toute personne ayant ou non une relation contractuelle avec le signataire ou avec le prestataire de services de certification"[250]. De même, selon la directive de l'Union européenne sur les 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 dans ce sens par tous les États membres, hormis deux[251].

200. 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, en matière de fourniture de services de certification, qu'un prestataire de services de certification est lié par une obligation de diligence à l'égard de quiconque peut être appelé à faire fond sur ses certificats pour décider s'il accepte une signature électronique déterminée dans une transaction donnée, vu que l'objet même de la délivrance du certificat est d'encourager une telle pratique"[252].

201. 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, ou dans certains pays, même des affirmations dont l'inexactitude est due à la négligence sont considérées comme des exceptions à la règle des pertes économiques[253] 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 sur les signatures électroniques. Ce sont par conséquent des règles usuelles de responsabilité qui s'appliquent, lesquelles sont en l'occurrence fondées sur le critère de proximité du préjudice[254].Le montant du préjudice pouvant donner lieu à réparation est une question réglée par le droit général de la responsabilité contractuelle ou le droit de la responsabilité délictuelle. Certaines législations font aux prestataires de services de certification 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[255].

---

[250]*Loi type de la CNUDCI sur les signatures électroniques…*, paragraphe 150.

[251]Les exceptions sont le Danemark et la Hongrie (Balboni, "Liability of certification service providers …", page 220.

[252]Lorna Brazell, Electronic Signatures: Law and Regulation (Londres, Sweet and Maxwell, 2004), page 187.

[253]Smedinghoff, "Certification authority: liability issues"…, section 4.5.

[254]Dumortier *et al*., "The legal and market aspects of electronic signatures"…, page 215.

[255]Turquie, Loi relative aux signatures électroniques, 2004, article 13; et Argentine, *Ley de firma digital (2001)*, alinéa *a* du paragraphe 1 de l'article 21 voir également Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (III).

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

202. Bien entendu, les prestataires de services de certification s'efforcent, 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 à la responsabilité par incident, par série d'incidents ou par période de temps, ou peuvent exclure certaines catégories de dommages. Une autre méthode consiste à indiquer dans les certificats la valeur maximale des transactions pour lesquelles ils peuvent être utilisés, ou à limiter l'utilisation des certificats à certaines fins exclusivement[256].

203. 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 droit romains, par exemple, il n'est pas possible pour une personne d'exclure totalement sa responsabilité du chef d'actes qui lui sont directement imputables[257] ou bien une telle exclusion est sujette à des limitations clairement stipulées[258]. De plus, si les conditions du contrat ne sont pas librement négociées mais s'il s'agit plutôt de conditions imposées ou préétablies par l'une des parties (contrat d'adhésion), certains types de clauses de restrictions peuvent être jugés "abusifs" et par conséquent frappés de nullité.

204. 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 ne conclurait et, d'un autre côté, aucune personne juste et honnête n'accepterait"[259] et qui sont caractérisées par "une absence de choix

---

[256]Voir Smedinghoff, "Certification authority: liability issues", section 5.2.5.4; et Hindelang, "No remedy for disappointed trust …", section 4.1.1.

[257]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" …n[os] 262 et 263).

[258]Dans la plupart des pays de droit romain, 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 paragraphe 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), page 217).

[259]*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", section 5.2.5.4.

authentique de la part de l'une des parties et par des conditions léonines en faveur de l'autre"[260]. Comme le concept de contrat d'adhésion que l'on trouve en droit civil, 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"[261]. 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[262].

205. Enfin, dans les pays de droit romain tout comme dans ceux 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.

206. 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 dans la plupart des cas sujette 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[263], 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 dûment informer 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 plus encore sans doute 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[264]. Beaucoup, en particulier parmi les représentants de l'industrie de la certification, ont considéré qu'il

---

[260]*First Financial Ins. Co.* c. *Purolator Security, Inc.*, citant *Williams* c. *Walker-Thomas Furniture Co.,* 350 F.2d 315, 320 (D.C. 1965), cité dans Smedinghoff, "Certification authority: liability issues"…, section 5.2.5.4.

[261]*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"…, section 5.2.5.4.

[262]Raymond T. Nimmer, *Information Law*, section 11.12[4][a], pages 11 à 37, cité dans Smedinghoff, "Certification authority: liability issues", section 5.2.5.4.

[263]Comme envisagé pour la E-Authentication Federation sous la houlette de l'Administration of the United States Government [voir E-Authentication Federation, Interim Legal Document Suite, version 4.0.7, accessible sur le site Internet: http://www.cio.gov/eauthentication/documents/LegalSuite.pdf (consulté le 6 juin 2008)].

[264]Sneddon, "*Legal liability and e-transactions …*"…, page 18.

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 de leur responsabilité.

207. Le désir d'élucider le droit dans ce domaine a conduit plusieurs pays à reconnaître expressément le droit des prestataires de services de certification à 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 s'assurer que le prestataire de services de certification indique "dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers"[265]. Ces limites peuvent habituellement être classées en deux catégories: il peut y avoir des restrictions concernant les types de transactions pour lesquelles peuvent être utilisés des certificats ou catégories de certificats déterminés; et il peut aussi y avoir des restrictions 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 eu égard au "préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation[266]. En outre, la directive de l'Union européenne sur les signatures électroniques impose aux États membres de l'Union de veiller à ce qu'un prestataire de services de certification "puisse indiquer, dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers"[267]. En pareil cas, "le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale"[268].

208. La directive de l'Union européenne sur les signatures électroniques 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 maximale de la transaction pour laquelle un certificat peut être utilisé, l'exonérant ainsi de responsabilité au-delà de ce plafond de valeur[269]. Il est fréquent aussi, dans la pratique commerciale, que les prestataires de services de certification introduisent par le biais de dispositions contractuelles un plafond global de leur responsabilité.

209. Les législations internes de plusieurs autres pays appuient 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 limites spécifiées dans l'énoncé des pratiques applicables par le prestataire de services de certification et, dans certains cas, exonèrent expressément

---

[265]Directive européenne sur les signatures électroniques, paragraphe 3 de l'article 6.

[266]Directive européenne sur les signatures électroniques… .

[267]Directive européenne sur les signatures électroniques, article 6, paragraphe 4 .
Directive européenne sur les signatures électroniques …

[268]Ibid.

[269]Dumortier *et al*., "The legal and market aspects of electronic signatures", page 55; voir aussi Hindelang, "No remedy for disappointed trust …", section 4.1.1; Balboni ("Liability of certification service providers …", page 230) va plus loin et affirme qu'"en vertu du paragraphe 4 de l'article 6 il n'est possible que de limiter la valeur de la transaction [...], ce qui n'a rien à voir avec une limite de la valeur potentielle du préjudice pouvant résulter de la transaction".

celui-ci de responsabilité lorsqu'un certificat a été utilisé à une fin autre que celle pour laquelle il a été délivré[270]. De plus, certains pays reconnaissent le droit des prestataires de services de certification d'émettre diverses catégories de certificats et d'établir des degrés de fiabilité recommandés différents[271], ce qui entraîne habituellement des niveaux variables 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 limite à l'utilisation ou à la valeur des certificats[272].

210. Les pays qui ont adopté une approche minimaliste, quant à eux, ont considéré une intervention du législateur comme généralement non souhaitable et ont préféré laisser aux parties le soin de régler la question dans leur contrat[273].

2. Cas particuliers de responsabilité dans le contexte d'une infrastructure à clef publique

211. Le débat touchant la responsabilité liée à l'utilisation de méthodes de signature et d'authentification électroniques a porté surtout sur les fondements et les caractéristiques de la responsabilité des prestataires de services de certification. L'on considère généralement que l'obligation principale d'un prestataire de services de certification est d'utiliser des systèmes, des procédures et des ressources humaines fiables et d'agir conformément aux politiques et aux pratiques qu'il a lui-même annoncées[274]. En outre, le prestataire de services de certification est censé faire preuve d'une diligence raisonnable pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat sont exactes et complètes. Toutes ces activités peuvent exposer le prestataire de services de certification à divers degrés de responsabilité, selon le droit applicable. L'on trouvera dans les paragraphes ci-après une série d'exemples de cas qui risquent d'exposer un prestataire de services de certification à une responsabilité accrue, ainsi qu'un résumé du régime appliqué par les législations nationales à ce type de responsabilité.

a) Absence d'émission ou émission tardive d'un certificat

212. Habituellement, un prestataire de services de certification délivre un certificat à la demande du signataire intéressé. Si la demande répond aux critères du prestataire

[270]Argentine, *Ley de firma digital (2001)*, article 39; Barbades, chapitre 308B, *Electronic Transactions Act, 1998,* section 20, paragraphes 3 et 4; Bermude, *Electronic Transactions Act*, *1999*, section 23, paragraphes 3 et 4; Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 14; et Viet Nam, Loi relative aux transactions électroniques, article 29, paragraphes 7 et 8 (dans ce dernier cas, cependant, sans exonération expresse de responsabilité).

[271]Singapour, *Electronic Transactions Act*, 1998, chapitre 88, sections 44 et 45; et Maurice, *Electronic Transactions Act*, 2000, articles 38 et 39.

[272]Turquie, Loi relative aux transactions électroniques, 2004, article 13.

[273]Voir, pour l'Australie, Sneddon, *Legal liability and e-transactions*…, pages 44 à 47; et pour les USA, Smedinghoff, "Certification authority: liability issues"…, section 5.2.51.

[274]Loi type de la CNUDCI sur les signatures électroniques …, alinéas *a* et *b* du paragraphe 1 de l'article 9.

de services, celui-ci peut émettre un certificat. Il est néanmoins concevable qu'une demande répondant aux critères fixés soit rejetée ou retardée, à la suite d'une simple erreur du prestataire de services de certification, ou bien parce que, délibérément ou par accident, le mécanisme de demande du prestataire de services n'est pas disponible, ou bien encore parce que, pour des raisons qui lui sont propres, le prestataire de services souhaite retarder ou refuser l'émission d'un certificat au demandeur. En pareilles circonstances, l'auteur d'une demande refusée ou retardée peut parfois se retourner contre le prestataire de services de certification[275].

213. Si plusieurs prestataires de services se font concurrence sur un même marché, le refus par tel ou tel prestataire de services d'émettre un certificat, que ce soit par accident ou délibérément, peut ne pas entraîner de réel préjudice pour le demandeur. Cependant, en l'absence d'une réelle concurrence, le refus d'émission ou l'émission tardive d'un certificat par un prestataire de services peut causer un sérieux préjudice si, en l'absence de certificat, le demandeur se voit dans l'impossibilité d'entreprendre l'affaire envisagée. Même si d'autres prestataires de services sont disponibles, il peut se produire un dommage spécifique lorsqu'un certificat a été demandé pour une transaction déterminée et que, l'émission du certificat ayant été refusée ou celui-ci ayant été émis tardivement, le demandeur n'a pas pu mener à bien la transaction potentiellement rémunératrice pour lui[276].

214. Ce type de situation est peu vraisemblable dans un contexte international, étant donné que la plupart des signataires ont généralement recours à des prestataires de services de certification établis dans leurs propres pays.

b) Négligence dans l'émission d'un certificat

215. Un certificat a censément pour fonction principale de lier l'identité du signataire à une clef publique. Aussi le principal devoir d'un prestataire de services de certification est-il de vérifier, conformément à ses pratiques officielles, que le demandeur est effectivement le signataire et qu'il contrôle la clef privée correspondant à la clef publique indiquée sur le certificat. Un manquement à cette tâche risque d'engager la responsabilité du prestataire de services de certification envers le signataire ou un tiers qui fait fond sur le certificat.

216. Le signataire peut subir un préjudice, par exemple, si un certificat est délivré par erreur à un imposteur utilisant une identité usurpée. Il se peut aussi que des employés ou des sous-traitants du prestataire de services lui-même s'entendent pour délivrer de faux certificats en utilisant la clef de signature du prestataire de services pour certifier des demandes injustifiées de l'imposteur. Il se peut en outre que ces personnes établissent par négligence un certificat erroné, soit en ne suivant pas comme il convient les procédures de validation officielle du prestataire de services de certification pour analyser la demande d'un imposteur, soit en utilisant la clef de signature du prestataire de

[275]Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

[276]Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

services pour créer un certificat qui n'a pas été approuvé. Enfin, il se peut qu'un malfaiteur usurpe l'identité d'un signataire en utilisant des documents d'identité falsifiés et apparemment authentiques et réussisse à convaincre le prestataire de services de lui délivrer un certificat, ceci dans le plein respect des politiques officielles de l'émetteur et en l'absence de faute quelconque[277].

217. La délivrance erronée d'un certificat à un imposteur peut avoir de très graves conséquences. Les parties qui réalisent des transactions en ligne avec l'imposteur risquent de faire fond sur les données inexactes figurant sur le certificat établi irrégulièrement et, ayant ainsi donné leur confiance, d'expédier les marchandises, virer des fonds, accorder un crédit ou entreprendre toute autre opération dans la conviction qu'elles traitent avec la partie dont l'identité a été usurpée. Lorsque la fraude est découverte, les parties qui ont fait fond sur le certificat risquent d'avoir subi un préjudice très substantiel. En pareil cas, il y a deux parties lésées: la partie qui a été amenée à faire fond sur le certificat délivré irrégulièrement et la personne dont l'identité a été usurpée. L'une et l'autre pourront se retourner contre le prestataire de services de certification. Une autre situation peut être celle d'un certificat délivré par négligence à une personne fictive, auquel cas seule la partie ayant accordé crédit au certificat subirait un dommage[278].

218. L'article 8 de la Loi type de la CNUDCI sur les signatures électroniques stipule notamment qu'un prestataire de services de certification prend des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes. Cette obligation de caractère général a été transposée mot pour mot dans la législation interne de plusieurs pays ayant appliqué la Loi type[279] encore que, dans certains pays, la norme fondée sur le caractère raisonnable des dispositions à prendre semble avoir été élevée[280].

219. Le régime établi par la directive de l'Union européenne sur les signatures électroniques fait obligation aux États membres de l'Union de veiller "au moins", à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat, soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de: *a)* l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié; *b)* l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données correspondant à la création de signature correspondant

[277]Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

[278]Smedinghoff, "Certification authority: liability issues" …, section 3.2.1.

[279]Par exemple, Thaïlande, *Electronic Transactions Act*, *2001*, section 28, paragraphe 2; et Îles Caïmanes (territoire britannique d'outremer), *Electronic Transactions Act*, *2000*, article 28 *b*.

[280]Par exemple, Chine, Loi relative aux transactions électroniques, article 22: "Les prestataires de services électroniques de certification doivent veiller à ce que le contenu des certificats de signature électronique soient complets et exacts pendant tout leur cycle de vie et faire en sorte que les parties qui s'en remettent aux signatures électroniques puissent vérifier ou comprendre l'intégralité du contenu des certificats et les autres questions pertinentes" (non souligné dans le texte).

aux données afférentes aux données de vérification de signature fournies ou identifiées dans le certificat; et *c)* l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification génère ces deux types de données. Cette responsabilité s'entend sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence[281].

220. Les législations d'autres pays s'accordent généralement pour imposer aux prestataires de services de certification l'obligation de vérifier l'exactitude des informations sur la base desquelles un certificat est délivré. Dans certains pays, le prestataire de services est généralement tenu pour responsable à l'égard de toute personne qui a raisonnablement fait fond sur l'exactitude de toutes les informations figurant sur le certificat accrédité, à compter de la date à laquelle celui-ci a été établi[282], ou de la date à laquelle la véracité de cette information a été garantie[283], bien que, pour certains droits nationaux, le prestataire de services puisse limiter sa responsabilité en insérant dans le certificat une mention appropriée[284]. Toutefois, la législation de certains pays exonère expressément le prestataire de services de certification de responsabilité du fait de l'inexactitude des informations fournies par le signataire, sous réserve de contrôle conformément aux pratiques applicables aux certificats, aussi longtemps qu'il peut apporter la preuve qu'il a pris toutes les mesures raisonnables pour vérifier les informations[285].

221. D'autres pays parviennent au même résultat non par une garantie légale, mais en imposant aux prestataires de services de certification l'obligation générale de vérifier les informations fournies par le signataire avant d'établir un certificat[286], ou d'établir des systèmes permettant de vérifier ces informations[287]. Dans certains cas, le prestataire de services est tenu de révoquer immédiatement le certificat s'il constate que les informations sur la base desquelles celui-ci a été établi étaient inexactes ou fausses[288]. Parfois, cependant, la loi est muette sur la délivrance des certificats, se bornant à stipuler que le prestataire de services de certification doit se conformer à

---

[281]Directive européenne sur les signatures électroniques, paragraphe 1 de l'article 6.

[282]Barbades, *Electronic Transactions Act, 1998*, alinéa *a* du paragraphe 1 de l'article 20, chapitre 308B; Bermude, *Electronic Transactions Act, 1999*, article 23; Hong Kong (Région administrative spéciale, (SAR) de Chine), *Electronic Transactions Ordinance*, article 39; Inde, Loi relative aux transactions électroniques, 2000, alinéa *e* de l'article 36; Maurice, *Electronic Transactions Act, 2000*, alinéa *d* du paragraphe 2 de l'article 27; et Singapour, *Electronic Transactions Act*, alinéas *a* et *c* du paragraphe 2 de l'article 29 et paragraphe 1, de l'article 1.

[283]Tunisie, *Loi relative aux échanges et au commerce électroniques*, article 18; et Viet Nam, Loi relative aux transactions électroniques, alinéa *d* de l'article 31.

[284]Par exemple, Barbades, Bermude, Hong Kong (SAR), Maurice et Singapour.

[285]Argentine, *Ley de firma digital (2001)*, paragraphe *c)* de l'article 39.

[286]Argentine, *Ley de firma digital (2001)*, alinéa *o* de l'article 21; Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma*, alinéa *e* de l'article 12; Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 104 (I); et Venezuela (République bolivarienne de), *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[287]Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, paragraphe d) de l'article 30.

[288]Argentine, *Ley de firma digital (2001)*, alinéa *e* du paragraphe 2 de l'article 19.

ses pratiques déclarées[289] ou délivrer le certificat comme convenu avec le signataire[290]. Cela ne signifie pas que la loi exonère totalement de responsabilité les prestataires de services de certification. Au contraire, la législation de certains États réglemente expressément la responsabilité des prestataires de services de certification en exigeant de ceux-ci qu'ils contractent une police d'assurance aux tiers adéquate pour couvrir tous les dommages contractuels et quasi délictuels causés à des signataires et à des tiers[291].

222. L'obligation du prestataire de services de certification de vérifier l'exactitude des informations communiquées est complétée par celle qu'a le signataire "de prendre, lorsqu'un certificat est utilisé pour étayer la signature électronique, des dispositions raisonnables pour assurer que toutes les déclarations essentielles qu'il fait concernant le certificat durant tout son cycle de vie ou devant figurer dans le certificat sont exactes et complètes"[292]. Le signataire pourrait par conséquent être tenu pour responsable à l'égard du prestataire de services de certification et de la partie ayant fait fond sur le certificat s'il fournit des informations fausses ou inexactes au prestataire de services lorsqu'il a demandé l'émission d'un certificat. Parfois, ce principe est présenté sous forme d'une obligation générale de communiquer des informations exactes au prestataire de services de certification[293] ou de prendre toutes les mesures raisonnables pour garantir l'exactitude des informations fournies[294]; le signataire est dans certains cas expressément tenu pour responsable des dommages résultant de son inobservation de cette obligation spécifique[295].

c) Utilisation non autorisée de signature ou déclaration de pratique de certification compromises

223. La question de l'utilisation non autorisée de dispositifs de création de signature et de certificats comporte deux aspects. D'une part, il se peut qu'un dispositif de création de signature ne soit pas conservé en lieu sûr ou, de quelque autre manière, soit compromis, par exemple si un agent du signataire s'en est indûment saisi. D'un autre côté, la hiérarchie de signature effective du prestataire de services de certification peut être devenue peu fiable, par exemple si la clef de signature ou la clef source du

---

[289]Pérou, *Decreto reglamentario de la ley de firmas y certificados digitales*, alinéa *a* de l'article 29.

[290]Colombie, *Ley 527 sobre comercio electrónico*, alinéa *a* de l'article 32; République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, alinéa *a* de l'article 40; et Panama, *Ley firma digital (2001)*, paragraphe 7 de l'article 49,.

[291]Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas*, article 32.

[292]Loi type de la CNUDCI sur les signatures électroniques …, alinéa *c* du paragraphe 1 de l'article 8.

[293]Argentine, *Ley de firma digital (2001)*, article 25; Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; et Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III).

[294]Îles Caïmanes, *Electronic Transactions Acts, 2000*, alinéa *c* de l'article 31.

[295]Colombie, *Ley 527 sobre comercio electrónico*, article 40; République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (III); et Panama, *Ley de firma digital (2001)*, article 39.

prestataire de services est perdue, divulguée à des personnes non autorisées ou utilisée par de telles personnes ou est compromise pour toute autre raison.

224. La hiérarchie de signature peut se trouver compromise de différentes façons. Il se peut que le prestataire de services de certification ou l'un de ses employés ou sous-traitants détruise la clef ou en perde le contrôle par inadvertance, que le centre de données détenant la clef privée soit endommagé par un accident ou que la clef du prestataire de services de certification soit délibérément détruite ou détournée à des fins illicites (par exemple par un pirate). Cette atteinte à l'intégrité de la hiérarchie de signature peut avoir de très graves conséquences. Par exemple, si la clef de signature privée ou les clefs sources tombent entre les mains d'un malfaiteur, celui-ci pourrait générer de faux certificats et les utiliser pour assumer l'identité de signataires réels ou fictifs, au détriment des parties qui croient en l'intégrité de la signature. De plus, une fois les dommages découverts, tous les certificats établis par les prestataires de services en question devraient être révoqués, ce qui pourrait entraîner un déluge de réclamations de la part de l'ensemble de la communauté des signataires pour perte d'usage.

225. Cette question n'est pas traitée en détail dans la Loi type de la CNUDCI sur les signatures électroniques. Certes, l'obligation générale qu'a le prestataire de services de certification d'utiliser, en vertu de la Loi type, "des systèmes, des procédures et des ressources humaines fiables"[296] peut être interprétée comme lui imposant l'obligation de prendre toutes les mesures nécessaires pour empêcher que sa propre clef (et par conséquent l'ensemble de la hiérarchie de signature) se trouve compromise. La législation interne de plusieurs États prévoit expressément une telle obligation, laquelle est fréquemment combinée à celle qui est imposée au prestataire de services de certification d'utiliser des systèmes fiables[297]. Parfois, la législation impose une obligation spécifique d'adopter des mesures pour éviter la falsification des certificats[298]. Le prestataire de services de certification a l'obligation de s'abstenir de créer les données afférentes à la création de signature des signataires ou d'y avoir accès, et peut voir sa responsabilité engagée si ses employés le font délibérément[299]. Si ses données afférentes à la création de signature étaient compromises, le prestataire de services de certification aurait l'obligation de demander la révocation de son propre certificat[300].

226. Le signataire, quant à lui, a également l'obligation de prendre toutes les précautions possibles. Aux termes de la Loi type de la CNUDCI sur les signatures électroniques, par exemple, le signataire "prend des dispositions raisonnables pour éviter toute utilisation non autorisée de ses données afférentes à la création de signature"[301]. Une

---

[296] Alinéa *f* du paragraphe 1 de l'article 9.

[297] Argentine, *Ley de firma digital (2001)*, alinéas *c* et *d* de l'article 21; Colombie, *Ley 527 sobre comercio electrónico*, alinéa *b* de l'article 32; Maurice, *Electronic Transactions Act, 2000*, article 24; Panama, *Ley de firma digital (2001)*, paragraphe 5 de l'article 49; Thaïlande, *Electronic Transactions Act (2001)*, paragraphe 6 de l'article 28; et Tunisie, *Loi relative aux échanges et au commerce électroniques*, article 13.

[298] Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas*, article 35.

[299] Argentine, *Ley de firma digital (2001)*, alinéa *b* de l'article 21.

[300] Argentine, *Ley de firma digital (2001)*, alinéa *p* de l'article 21.

[301] Alinéa *a* du paragraphe 1 de l'article 8.

obligation semblable est imposée par la législation interne de la plupart des États, bien qu'avec certaines variantes. Parfois, la loi impose au signataire l'obligation rigoureuse de conserver le contrôle exclusif des dispositifs de création de signature et d'empêcher qu'ils soient utilisés sans autorisation[302], ou rend le signataire exclusivement responsable de la bonne garde du dispositif de création de signature[303]. Fréquemment, toutefois, cette obligation est nuancée et consiste simplement à maintenir le contrôle adéquat sur le dispositif de création de signature ou à adopter les mesures appropriées pour en conserver le contrôle[304], à faire preuve de diligence pour éviter qu'il soit utilisé sans autorisation[305], ou à prendre des mesures raisonnables pour éviter que son dispositif de signature soit utilisé sans autorisation[306].

d) Non-suspension ou non-révocation d'un certificat

227. Le prestataire de services de certification peut également voir sa responsabilité engagée s'il s'abstient de suspendre ou de révoquer un certificat compromis. Si l'on veut qu'une infrastructure de signatures numériques fonctionne correctement et inspire confiance, elle doit impérativement être dotée d'un mécanisme permettant de déterminer en temps réel si tel ou tel certificat est valable ou s'il a été suspendu ou révoqué. Lorsqu'une clef privée est compromise, par exemple, la révocation du certificat constitue le principal mécanisme grâce auquel le signataire peut se protéger contre les transactions frauduleuses entreprises par des imposteurs pouvant avoir obtenu copie de sa clef privée.

228. De ce fait, la rapidité avec laquelle le prestataire de services de certification révoque ou suspend un certificat du signataire à la demande de celui-ci revêt une importance critique. Le laps de temps qui s'écoule entre la demande de révocation d'un certificat présentée par un signataire, sa révocation effective et la publication de l'avis de révocation peut permettre à un imposteur de mener à bien sa transaction frauduleuse. En conséquence, si le prestataire de services de certification tarde de façon déraisonnable à mentionner la révocation sur la liste de certificats révoqués ou omet

---

[302] Argentine, *Ley de firma digital (2001)*, alinéa *a* de l'article 25; Colombie, *Ley 527 sobre comercio electrónico*, paragraphe 3 de l'article 39; Fédération de Russie, Loi fédérale sur les signatures numériques électroniques (2002), paragraphe 1 de la clause 12; Panama, *Ley de firma digital (2001)*, paragraphe 4 de l'article 37; République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, alinéa *d* de l'article 53; et Turquie, Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la loi de 2005 relative aux signatures électroniques (2005), alinéa *e* de l'article 15.

[303] Tunisie, *Loi relative aux échanges et au commerce électroniques*, article 21.

[304] Chili, *Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (2002)*, article 24; et Viet Nam, Loi sur les transactions électroniques, alinéa *a* du paragraphe 2 de l'article 25.

[305] Venezuela (République bolivarienne du) , *Ley sobre mensajes de datos y firmas electrónicas*, article 19.

[306] Îles Caïmanes, *Electronic Transactions Act, 2000*, alinéa *a* article 39; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, alinéa *b* de l'article 17; Inde, *Information Technology Act, 2000*, paragraphe 1 de l'article 42; Maurice, *Electronic Transactions Act 2000*, alinéas *a* et *b* du paragraphe 1 de l'article 35; Mexique, *Código de Comercio: Decreto sobre firma electrónica (2003)*, article 99 (II); Singapour, *Electronic Transactions Act* (chapitre 88), section 39; et Thaïlande, *Electronic Transactions Act (2001)*, paragraphe 1 de l'article 27.

de le faire, aussi bien le signataire que la partie lésée qui a fait fond sur les signatures risquent de subir un sérieux préjudice pour s'être fiés à un certificat apparemment valable. En outre, les prestataires de services de certification peuvent, dans le cadre des services qu'ils offrent, proposer aussi de tenir des répertoires et des listes de certificats révoqués auxquels les parties pourront avoir accès. L'administration d'une telle base de données comporte un double risque: le risque que le répertoire ou la liste de certificats révoqués soient inexacts, ce qui peut conduire la partie qui les consulte à faire fond à ses dépens sur des informations erronées; et le risque que le répertoire ou la liste de certificats révoqués ne soient pas disponibles (par exemple par suite d'une panne du système), empêchant ainsi les signataires et les parties se fiant au certificat correspondant de mener à bien leurs transactions.

229. Comme indiqué ci-dessus, la Loi type de la CNUDCI sur les signatures électroniques prend pour hypothèse que le prestataire de services de certification peut émettre des certificats de niveaux divers, caractérisés par des degrés divers de fiabilité et de sécurité. En conséquence, la Loi type n'impose pas toujours à un prestataire de services l'obligation de mettre en place un système de révocation, ce qui pourrait ne pas être commercialement viable pour certains types de certificats de faible valeur. La Loi type se borne donc à stipuler que le prestataire de services de certification doit fournir "des moyens raisonnablement accessibles" pour permettre à toute partie se fiant au certificat de déterminer à partir de celui-ci, entre autre, s'il existe des moyens pour le signataire d'adresser une notification indiquant que les données de création de la signature ont été compromises et si un service de révocation en temps utile est offert[307]; lorsqu'un tel service de révocation en temps utile est offert, le prestataire de services de certification a l'obligation de veiller à ce qu'il soit disponible[308].

230. Le régime établi par la directive de l'Union européenne sur les signatures électroniques fait obligation aux États membres de l'Union de veiller "au moins", à ce qu'un prestataire de services de certification qui délivre à l'intention du public un certificat présenté comme qualifié soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat s'il n'a pas publié la révocation de celui-ci, à moins que le prestataire de services de certification prouve qu'il n'a pas agi par négligence[309]. Certains droits internes contraignent le prestataire de services de certification à adopter des mesures pour prévenir la falsification des certificats[310] ou pour révoquer immédiatement un certificat dès qu'il apprend que les informations sur la base desquelles le certificat a été émis étaient inexactes ou fausses[311].

231. Le signataire et les autres personnes autorisées peuvent également être soumis à une obligation semblable. La Loi type de la CNUDCI sur les signatures électroniques, par exemple, stipule que chaque signataire doit utiliser sans retard injustifié les moyens fournis par le prestataire de services de certification, ou faire d'une autre

---

[307]Sous-alinéas v et vi de l'alinéa *d* du paragraphe 1 de l'article 9.

[308]Alinéa *e* du paragraphe 1 de l'article 9.

[309]Directive européenne sur les signatures électroniques…, paragraphe 2 de l'article 6; voir aussi alinéa *b* de l'annexe II de la directive.

[310]Panama, *Ley de firma digital (2001)*, paragraphe 6 de l'article 49.

[311]Argentine, *Ley de firma digital (2001)*, alinéa *e* du paragraphe 2 de l'article 19.

manière des efforts raisonnables pour aviser toute personne dont il peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique, s'il sait que les données afférentes à la création de signature ont été compromises ou s'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[312].

232. Les législations nationales stipulent fréquemment que le signataire a l'obligation de demander la révocation du certificat en toute circonstance où la confidentialité des données de création de signature risque d'avoir été compromise[313], bien que, dans certains cas, les signataires soient simplement tenus de communiquer ce fait au prestataire de services de certification[314]. Les législations de plusieurs États ont adopté la formulation figurant dans la Loi type de la CNUDCI sur les signatures électroniques, qui fait au signataire l'obligation d'aviser toute personne dont le signataire du dispositif de signature peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique[315]. Les législations de plusieurs États ont adopté la formulation figurant dans la Loi type de la CNUDCI sur les signatures électroniques, qui fait au signataire l'obligation d'aviser toute personne dont le signataire du dispositif de signature peut raisonnablement penser qu'elle se fie à la signature électronique ou qu'elle fournit des services visant à étayer la signature électronique[316].

Conclusion

233. L'utilisation de plus en plus généralisée des méthodes d'authentification et de signature électroniques pourra beaucoup contribuer à réduire la documentation commerciale et les coûts connexes afférents aux transactions internationales. Alors que, dans une très large mesure, le rythme du progrès dans ce domaine dépendra de la

[312]Sous-alinéas i et ii de l'alinéa *b* du paragraphe 1 de l'article 8.

[313]Argentine, *Ley de firma digital (2001)*, alinéa *c* de l'article 25; Colombie, *Ley 527 sobre comercio electrónico*, paragraphe 4 de l'article 39; République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 49 et alinéa *e* de l'article 53; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, alinéa *f* de l'article 17; Fédération de Russie, Loi fédérale sur les signatures numériques électroniques (2002), paragraphe 1 de la clause 12; Maurice, *Electronic Transactions Act, 2000*, article 36; Panama, *Ley de firma digital (2001)*, paragraphe 5 de l'article 37; et Singapour, *Electronic Transactions Act* (chapter 88), section 40.

[314]Inde, *Information Technology Act, 2000*, paragraphe 2 de l'article 42; et Turquie, Ordonnance relative aux procédures et principes applicables à la mise en œuvre de la loi de 2005 relative aux signatures électroniques (2005), alinéas *f* et *i* de l'article 15.

[315]Îles Caïmanes, *Electronic Transactions Act, 2000*, alinéa *b* de l'article 15; Chine, Loi relative aux signatures électroniques, article 15; Thaïlande, *Electronic Transactions Act (2001)*, paragraphe 2 de l'article 27; et Viet Nam, Loi sur les transactions électroniques, alinéa *b* du paragraphe 2 de l'article 25.

[316]Chine, Loi relative aux signatures électroniques, article 27; République dominicaine, *Ley sobre comercio electrónico, documentos y firmas digitales (2002)*, article 55; Équateur, *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, alinéa *e* de l'article 17; Panama, *Ley de firma digital (2001)*, article 39; Fédération de Russie, Loi fédérale sur les signatures numériques électroniques (2002), paragraphe 2 de la clause 12; et Venezuela (République bolivarienne du), *Ley sobre mensajes de datos y firmas electrónicas*, article 40.

qualité et de la sécurité de solutions technologiques, le droit peut beaucoup faciliter l'utilisation des méthodes d'authentification et de signature électroniques.

234. Un grand nombre de pays ont déjà adopté des mesures nationales allant dans ce sens en promulguant des lois reconnaissant la valeur juridique des communications électroniques et en définissant les critères de leur équivalence avec les documents sur support papier. Les dispositions réglementant les méthodes électroniques d'authentification de signature constituent fréquemment un élément important de ces lois. La Loi type de la CNUDCI sur le commerce électronique est devenue l'instrument de référence le plus communément utilisé pour la promulgation de législations dans ce domaine et sa large application a contribué à fortement harmoniser les régimes applicables au plan international. Une large ratification de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux encouragerait encore plus le mouvement d'harmonisation en offrant une série déterminée de règles pour les transactions internationales.

235. L'utilisation au plan international des méthodes d'authentification et de signature électroniques pourrait aussi bénéficier de l'adoption de ces normes de la CNUDCI. En particulier, la souplesse des critères d'équivalence fonctionnelle entre signatures électroniques et signatures sur support papier, reflétée dans la Convention des Nations Unies sur l'utilisation des signatures électroniques dans les contrats internationaux, pourra offrir un cadre international commun permettant aux méthodes d'authentification et de signature électroniques de répondre aux exigences étrangères de forme des signatures. Néanmoins, il se peut que certains problèmes persistent, en particulier pour ce qui est de l'utilisation au plan international de méthodes d'authentification des signatures électroniques qui exigent la participation de tiers de confiance dans le processus d'authentification ou de signature.

236. Les problèmes qui se posent dans ce domaine spécifique découlent pour une très large part du manque de cohérence des normes techniques et de la non-compatibilité des matériels ou des logiciels, ce qui se traduit par un manque d'interopérabilité au plan international. Les efforts entrepris pour harmoniser les normes et améliorer la compatibilité technique pourront déboucher sur une solution aux difficultés qui existent actuellement. Néanmoins, il y a aussi des difficultés de caractère juridique liées à l'utilisation des méthodes électroniques d'authentification des signatures, en particulier dans le contexte des législations nationales qui, soit prescrivent, soit privilégient, l'emploi d'une technologie déterminée pour les signatures électroniques, habituellement les technologies de signature numérique.

237. Les législations qui reconnaissent la valeur juridique des signatures numériques n'attribuent habituellement la même valeur juridique aux signatures étayées par des certificats étrangers que dans la mesure où ceux-ci sont considérés comme équivalant à des certificats nationaux. Il ressort de la présente étude que, pour apprécier comme il convient l'équivalence juridique, il faut comparer non seulement les normes techniques et de sécurité qui caractérisent une technologie de signature déterminée, mais aussi les règles qui régiraient la responsabilité des différentes parties en cause. La Loi type de la CNUDCI sur les signatures électroniques contient une série de règles

fondamentales communes régissant certaines des obligations des parties qui interviennent dans le processus d'authentification et de signature, et qui peuvent avoir un impact sur leur responsabilité individuelle. Il existe en outre des textes de caractère régional, comme la directive de l'Union européenne sur les signatures électroniques, qui offrent un cadre législatif semblable pour définir le régime de responsabilité des prestataires de services de certification opérant dans la région. Cependant, aucun de ces textes ne se penche sur l'ensemble des questions de responsabilité découlant de l'utilisation au plan international de certaines méthodes d'authentification et de signature électronique.

238. Il est important que les législateurs et les décideurs saisissent bien les différences entre les régimes nationaux de responsabilité et les éléments qui leur sont communs, pour être en mesure de concevoir des méthodes et procédures appropriées en matière de reconnaissance de signatures étayées par des certificats étrangers. Les législations nationales de divers pays peuvent déjà apporter des réponses largement équivalentes aux diverses questions évoquées dans la présente publication, par exemple parce qu'elles partagent une tradition juridique commune ou appartiennent à un cadre d'intégration régionale. Il se peut que ces pays aient intérêt à mettre au point des normes communes de responsabilité ou même harmoniser leurs règles nationales, de manière à faciliter l'utilisation transfrontière des méthodes d'authentification et de signature électroniques.

كيفية الحصول على منشورات الأمم المتحدة

يمكن الحصول على منشورات الأمم المتحدة من المكتبات ودور التوزيع في جميع أنحاء العالم. استعلم عنها من المكتبة التي تتعامل معها أو اكتب إلى: الأمم المتحدة، قسم البيع في نيويورك أو في جنيف.

如何购取联合国出版物

联合国出版物在全世界各地的书店和经售处均有发售。 请向书店询问或写信到纽约或日内瓦的联合国销售组。

HOW TO OBTAIN UNITED NATIONS PUBLICATIONS

United Nations publications may be obtained from bookstores and distributors throughout the world. Consult your bookstore or write to: United Nations, Sales Section, New York or Geneva.

COMMENT SE PROCURER LES PUBLICATIONS DES NATIONS UNIES

Les publications des Nations Unies sont en vente dans les librairies et les agences dépositaires du monde entier. Informez-vous auprès de votre libraire ou adressez-vous à: Nations Unies, Section des ventes, New York ou Genève.

КАК ПОЛУЧИТЬ ИЗДАНИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ

Издания Организации Объединенных Наций можно купить в книжных магазинах и агентствах во всех районах мира. Наводите справки об изданиях в вашем книжном магазине или пишите по адресу: Организация Объединенных Наций, Секция по продаже изданий, Нью-Йорк или Женева.

CÓMO CONSEGUIR PUBLICACIONES DE LAS NACIONES UNIDAS

Las publicaciones de las Naciones Unidas están en venta en librerías y casas distribuidoras en todas partes del mundo. Consulte a su librero o diríjase a: Naciones Unidas, Sección de Ventas, Nueva York o Ginebra.

United Nations publication
ISBN: 978-92-1-233467-7
Sales No. F.09.V.4

FOR UNITED NATIONS USE ONLY

Printed in Austria
V.08-55699—March 2009—585