Cadre juridique pour les signatures électroniques et les services de certification

Gobert, Didier

Published in:
La preuve

Publication date:
2002

Document Version
le PDF de l'éditeur

Consult **& T**raining

G O B E R T SPRL

Droit de l'informatique et des réseaux

www.consultandtraining.com
didier.gobert@dgobert.be

a le plaisir de vous présenter :

Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001

Didier GOBERT

(Publié *in La preuve*, Formation permanente CUP, Volume 54, mars 2002, pp. 83 à 172.)

Publié *in La preuve*, Formation permanente CUP, Volume 54, mars 2002, pp. 83 à 172.

Cadre juridique pour les signatures électroniques et les services de certification : analyse de la loi du 9 juillet 2001

Didier GOBERT
Assistant au CRID (Université de Namur)
Consultant en droit de l'informatique (www.consultandtraining.com)

Introduction – contexte général

L'utilisation généralisée des technologies de l'information et de la communication permet aux individus et aux organisations de s'échanger diverses informations d'un coin du monde à l'autre, et ce à la vitesse de l'éclair. Plus besoin de se déplacer, plus besoin de s'entendre, plus besoin de se rencontrer. On assiste à un basculement progressif des relations entre les individus du monde traditionnel vers le monde virtuel.

Ce cadre enchanteur du « tout électronique », et l'apparence de liberté qui en découle, ne doit pas faire oublier que la confiance dans les relations humaines a souvent été bâtie au gré des rencontres entre partenaires potentiels et suite à la formalisation de leurs engagements éventuels sur un support papier – difficilement altérable – revêtu de notre « bonne veille » signature manuscrite. Comment maintenir un tel climat de confiance dans un monde virtuel dans lequel les parties ne se voient ni ne s'entendent et dans lequel l'aspect immatériel des échanges pose la question du caractère bien réel de ceux-ci, particulièrement dans les réseaux ouverts à tout venant ?

Dans ce contexte, il est rapidement apparu nécessaire de développer des techniques – ayant donné lieu à la création de ce que certains auteurs ont appelé les « nouveaux métiers de la confiance »[1] – permettant de gagner la confiance des utilisateurs afin d'assurer le développement harmonieux des échanges au sein des réseaux virtuels. Ces diverses techniques impliquent généralement l'intervention d'un tiers dont le métier est précisément de mettre en œuvre tous les moyens techniques afin de créer un contexte dans lequel les parties peuvent établir des échanges en toute sécurité. Dans le cadre de l'utilisation de signatures électroniques, ce tiers de confiance est appelé « prestataire de service de certification » (ci-après « PSC »).

Le législateur européen, repris en chœur par les législateurs nationaux, a probablement estimé que la confiance devait se mériter, ce qui a justifié l'adoption d'un régime juridique spécifique applicable aux activités des prestataires de service de certification. Ledit régime est établi par la directive européenne du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[2], transposée en droit belge par la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification[3].

Nous proposons de commenter de manière approfondie et méthodique cette loi du 9 juillet 2001 afin de préciser, dans une matière dominée par la complexité, la portée des différentes

[1] M. ANTOINE, D. GOBERT et A. SALAÜN, « Le développement du commerce électronique : les nouveaux métiers de la confiance » *in Droit des technologies de l'information-Regards prospectifs*, Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999, pp. 3-32.
[2] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000.
[3] *M.B.*, 29 septembre 2001, pp. 33070-33078.

dispositions et de relever le cas échéant les lacunes ou contradictions. Après avoir rappelé le rôle primordial joué par le PSC et les raisons qui justifient la réglementation des services offerts par ce dernier (section 1ère), nous présentons les trois principes généraux de la loi, précisons son champ d'application et décortiquons ses diverses définitions (section 2). Ensuite, nous abordons le régime juridique proprement dit des PSC en distinguant s'ils délivrent des certificats qualifiés ou non (section 3). Nous n'oublions pas d'exposer les droits et obligations applicables aux autres intervenants que sont les utilisateurs de certificats et l'Administration (section 4) pour, enfin, terminer par mettre en avant les conditions de la reconnaissance transfrontière des certificats qualifiés (section 5).

Afin de tracer les limites de cette contribution, il convient de préciser que deux points importants de la loi du 9 juillet 2001 ne sont pas traités ici. Il s'agit, d'une part, des principes relatifs à la reconnaissance juridique des signatures électroniques (spécialement l'article 4, §§ 4 et 5), d'autre part, de la question de la signature des personnes morales. Sur ces deux points, nous renvoyons respectivement à la contribution du Professeur Etienne Montero et à celle de Bernard Vanbrabant dans le présent ouvrage.

Section 1.
Le rôle du prestataire de service de certification et la nécessité de réglementer ses activités

Ce n'est pas le lieu de présenter les différentes techniques de signature électronique et leur fonctionnement respectif. Nous renvoyons le lecteur à la littérature abondante en cette matière[4]. Rappelons toutefois qu'à l'heure actuelle, la technique de signature numérique, fondée sur la cryptographie asymétrique et utilisée dans le cadre d'une infrastructure à clé publique, s'impose *de facto*. Celle-ci nécessite l'intervention d'un tiers de confiance, appelé prestataire de service de certification ou aussi autorité de certification.

Dans une infrastructure à clé publique, le PSC est un organisme indépendant dont la fonction principale consiste, d'une part, à *vérifier l'identité* des titulaires de clé publique[5] et à *générer des certificats* (sortes d'attestations électroniques qui établissent le lien entre une personne et sa clé publique[6]), d'autre part, à *assurer la publicité* la plus large des certificats ainsi émis[7]. Le

[4] S. PARISIEN et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Ed. Yvon Blais Inc., 1996 ; J. HUBIN, *La sécurité informatique, entre technique et droit*, Cahiers du C.R.I.D., n° 14, E. Story-Scientia, 1998 ; D. MOUGENOT, "Droit de la preuve et technologies nouvelles: synthèse et perspectives", *in Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, pp. 45-105 ; D. GOBERT et E. MONTERO, « La signature dans les contrats et les paiements électroniques : l'approche fonctionnelle », *DA/OR*, 2000, n° 53, pp. 17-39 ; A. JAMAR, « La sécurité des transactions – Introduction technique », *in Le commerce électronique : un nouveau mode de contracter ?*, Editions du jeune barreau de Liège, 2001, pp. 21 et s. ; T. VERBIEST et E. WERY, avec la collaboration de D. GOBERT et A. SALAÜN, *Le droit de l'Internet et de la société de l'information*, Bruxelles, Larcier, 2001, n° 684 et s.

[5] Notons que l'ensemble des certificats délivrés par un PSC ne sont pas nécessairement des certificats d'identité. Certains certificats peuvent être anonymes, viser des objets (serveur, logiciel) ou ne concerner que des attributs. Toutefois, dans la matière qui nous préoccupe, à savoir l'utilisation des certificats aux fins juridiques de signature, nous ne traiterons que des certificats d'identité.

[6] Cette clé publique ainsi que la clé privée complémentaire peuvent être générées soit par le titulaire du certificat soit par le PSC.

[7] Pour plus de détails, voy. S. PARISIEN et P. TRUDEL, *op. cit.*, pp. 117 et s.; E. DAVIO, "Certification, signature et cryptographie", in E. MONTERO (éd.), *Internet face au droit*, Cahiers du C.R.I.D., n° 12, E. Story-Scientia,

PSC est également tenu d'assurer au public un accès permanent au répertoire contenant les certificats de clé publique et de maintenir à jour celui-ci, en veillant, le cas échéant, à procéder à la révocation des certificats. En effet, l'accès au certificat de clé publique est indispensable pour permettre à toute personne destinatrice d'un message signé numériquement de vérifier la signature. En outre, le PSC peut remplir d'autres fonctions connexes à la certification d'identité : l'archivage des informations qui sont relatives aux certificats (notamment à des fins probatoires) ; la génération de la paire de clés ; la vérification de signatures numériques et la confirmation de leur validité[8].

Notons que si la délivrance de certificats constitue la fonction principale du PSC, celui-ci peut également offrir d'autres services tels que ceux d'horodatage et/ou de conservation des documents signés numériquement, d'émission de certificats d'attributs, de sécurisation et d'authentification de labels, etc.

Dès lors, on constate le rôle capital de ce tiers à la communication électronique pour assurer la fiabilité de la signature numérique et l'identification des intervenants, en vue d'échanges juridiquement contraignants dans les réseaux ouverts. Il doit mettre en place une infrastructure qui permette de vérifier et d'assurer la véracité et l'intégrité des informations utiles à la certification lors de la collecte, la conservation et l'émission de celles-ci. Le rôle du prestataire de service de certification dans la société de l'information est à ce point important qu'il a justifié l'adoption au niveau européen d'un régime juridique précis et unifié, transposé en droit belge par la loi du 9 juillet 2001[9].

Signalons que l'adoption de cette loi ne s'est pas faite sans mal. Le 16 décembre 1999, le gouvernement déposa devant la Chambre des représentants le projet de loi 322 relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques[10]. Ce texte pouvait difficilement constituer une transposition adéquate de la directive européenne sur les signatures électroniques puisque cette dernière ne fut adoptée que 3 jours auparavant et publiée le 19 janvier 2000[11] ! Conformément à la procédure européenne d'information qui instaure un mécanisme de transparence réglementaire dans le domaine des règles techniques (Directive 98/34/CE), le gouvernement a dû notifier le projet de loi à la Commission européenne. Suite à l'examen du projet dans le cadre de la procédure précitée, la Commission a émis un avis circonstancié le 10 mai 2000, invitant le gouvernement belge à transposer correctement la directive européenne. Afin de prendre en compte cet avis circonstancié et les observations formulées par la Commission européenne, un amendement remodelant complètement le texte fut déposé le 10 novembre 2000[12]. Après avoir été évoqué et amendé par le Sénat[13], le projet fut finalement adopté par la Chambre en séance plénière le

---

1997, pp. 80 et s. ; M. ANTOINE et D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.*, juillet-octobre 1998, n° 4/5, spéc. pp. 293 et s.

[8] S. PARISIEN et P. TRUDEL, *op.cit.*, pp. 128 à 130 ; E.A. CAPRIOLI, « Sécurité et confiance dans le commerce électronique : Signature numérique et autorité de certification », *La Semaine Juridique Edition Générale*, avril 1998, n°14, p.589.

[9] Loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, *M.B.*, 29 septembre 2001, pp. 33070-33078.

[10] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1, disponible à l'adresse suivante : http://www.lachambre.be/cgi-bin/docs.bat?l=f&dir=322

[11] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, L 13/12 à 20 du 19 janvier 2000.

[12] Amendement n° 1 du Gouvernement, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2.

[13] *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/1 à 7.

14 juin 2001[14], promulgué le 9 juillet et publié au Moniteur belge le 29 septembre de la même année.

La loi ne contenant aucune disposition sur son entrée en vigueur, on en conclut que celle-ci est en vigueur depuis le 9 octobre 2001. Néanmoins, précisons que certaines dispositions nécessitent des mesures d'exécution, dont l'article 4, § 3, qui permet au Roi de soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles ; l'article 7, § 3, qui charge le Roi de fixer les conditions auxquelles doivent répondre les organismes pour être jugés compétents pour attester la conformité des dispositifs sécurisés de création de signature électronique ; l'article 17, § 2, qui charge le Roi de fixer les conditions et modalités pour l'accréditation des prestataires de service de certification ; l'article 20, § 1er, qui charge le Roi de fixer les règles relatives au contrôle des prestataires de service de certification et enfin l'article 20, § 2, qui charge le Roi de fixer les conditions auxquelles l'Administration peut demander aux prestataires de service de certification les informations nécessaires à leur contrôle. Au moment où nous écrivions ces lignes, les arrêtés royaux d'exécution n'étaient toujours pas publiés.

Section 2.
Préliminaires : définitions, champ d'application et principes généraux de la loi

Le juriste non averti mais aussi le technicien familiarisé au fonctionnement de la cryptographie asymétrique peuvent éprouver quelques difficultés à saisir les réalités qui se cachent derrière les définitions inscrites dans l'article 2 de la loi. En raison du caractère technique et peu convivial de celles-ci, nous proposons de les commenter une à une. Ensuite nous précisons le champ d'application de la loi ainsi que les principes généraux qu'elle consacre.

A. Définitions

Conformément à la directive, et contrairement à l'avant-projet de loi soumis à l'avis du Conseil d'Etat[15], les définitions inscrites dans la loi montrent clairement qu'elles ne se limitent pas au mécanisme de signature digitale, fondé sur la cryptographie asymétrique. En effet, eu égard à la rapidité des progrès techniques et aux principes de concurrence, la loi adopte une approche qui essaye de prendre en compte les diverses technologies actuelles ou futures susceptibles d'assurer les fonctions d'identification, d'adhésion et d'intégrité. Ce principe de « neutralité technologique » apparaît clairement dans le considérant n° 8 de la directive européenne sur les signatures électroniques. Ainsi, les définitions adoptées se veulent les plus larges possibles afin de ne pas privilégier une technique particulière de signature électronique, même si on sait qu'actuellement la signature numérique (ou digitale) semble la plus mûre et s'imposer sur le marché.

On relève dans l'article 2 de la loi un dédoublement systématique de certaines définitions : signature électronique – signature électronique *avancée* ; certificat – certificat *qualifié* ;

[14] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/8.
[15] Avant-projet de loi relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1, pp. 44-55.

dispositif de création de signature[16] – dispositif *sécurisé* de création de signature. L'intérêt de ce dédoublement apparaît clairement dans les paragraphes 4 et 5 de l'article 4 : seules les techniques répondant aux conditions des secondes définitions bénéficient des effets privilégiés de la clause d'assimilation consacrée par l'article 4, § 4. Dans le cas contraire, seule la clause de non discrimination contenue dans l'article 4, § 5, s'applique. Sur ce point, nous renvoyons le lecteur à la contribution du professeur Etienne Montero dans ce même ouvrage.

Nous renvoyons également le lecteur à cette même contribution pour le commentaire des notions de signature électronique et de signature électronique *avancée* (art. 2, 1° et 2°) ainsi que pour la détermination de la portée de ces définitions sur la question de la reconnaissance juridique de la signature électronique en droit belge.

1. Titulaire de certificat (art. 2, 5°)

Dans son article 2, 5°, la loi définit le *titulaire de certificat* comme « une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat ».

Il apparaît clairement que le titulaire de certificat peut aussi bien être une personne physique que morale. Selon l'exposé des motifs, cette définition consacre le principe selon lequel un certificat peut être délivré à toute personne ayant la personnalité juridique (un citoyen, une société commerciale, une ASBL, une personne morale de droit publique, une EPA…) [17]. *A contrario*, cela exclut la délivrance d'un certificat, à tout le moins qualifié, à une association de fait, telle qu'un parti politique par exemple[18]. Par ailleurs, rien ne semble faire obstacle à ce qu'une personne physique ou morale devienne titulaire de plusieurs certificats, ayant le cas échéant des attributs différents, qu'elle utiliserait dans le cadre d'activités distinctes.

Le titulaire de certificat est la personne telle qu'identifiée dans le certificat. Il en résulte que les mentions relatives à l'identité, aux données afférentes à la vérification de signature ainsi qu'à l'éventuel attribut contenues dans le certificat, sont des mentions liées à la personne titulaire du certificat[19]. Celle-ci jouit des droits et obligations inscrits dans la loi.

Par contre, la notion de titulaire de certificat ne doit pas être confondue avec la notion – non consacrée par la loi – de détenteur des données afférentes à la création de signature. En effet, les données afférentes à la création de signature sont en pratique stockées sur un support matériel, tel qu'une carte à puce[20]. Or le titulaire de certificat, qui est également titulaire de ces données, n'est pas nécessairement détenteur de celles-ci. Ainsi, une personne morale est titulaire du certificat mais n'est pas détentrice de ce dernier et des données afférentes à la création de signature. N'existant pas matériellement, elle n'est pas capable de détenir celles-ci stockées sur la carte à puce et encore moins de les mettre en œuvre pour générer une

[16] La notion de « dispositif de création de signature » n'apparaît pas expressément dans la loi belge. Néanmoins, elle est consacrée par l'article 2, 5) de la directive et découle *a contrario* de la notion de « dispositif *sécurisé* de création de signature » (art. 2, 7°, de la loi) : un dispositif de création de signature n'est pas *sécurisé* lorsqu'il ne satisfait pas à l'ensemble des exigences de l'annexe III.

[17] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 19 et 20.

[18] Néanmoins, rien n'interdit à un membre d'un parti politique d'obtenir un certificat à son nom avec pour attribut sa fonction au sein du parti.

[19] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 20.

[20] Il ne s'agit ni d'une obligation ni du seul support possible. Mais la carte à puce offre un haut niveau de sécurité.

signature. Une personne physique – habilitée à représenter la société – est donc nécessairement détentrice de ces données[21].

Les droits et obligations stipulés par ou en vertu de la loi ne s'appliquent qu'au titulaire de certificat, et en aucun cas au détenteur de certificat[22]. Néanmoins, ce dernier n'agira pas en tout anonymat puisque l'article 8, § 3, fait obligation au PSC de tenir « un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique ». On notera que ce paragraphe 3 ne vise que l'hypothèse de la représentation d'une personne morale. Une obligation comparable ne semble pas exister pour l'éventuelle détention d'un certificat par une personne physique qui représenterait une autre personne physique.

Les conséquences de cette distinction « titulaire – détenteur de certificat », ainsi que la volonté de reconnaître la signature des personnes morales, justifient que la notion de « signataire » consacrée par la directive n'ait pas été reprise. Pourtant, un amendement déposé au Sénat proposait de compléter la liste des définitions en y ajoutant la notion de signataire[23]. Le ministre demanda de rejeter l'amendement – avec succès – au motif que la loi concerne les droits et obligations ainsi que la responsabilité du titulaire du certificat et non pas du signataire. Le ministre explique qu'en pratique, la notion de titulaire de certificat est plus précise que celle de signataire. De plus, il peut y avoir, toujours selon le ministre, une différence entre le titulaire de certificat et le signataire. En effet, dans le cas où le titulaire est une personne morale, il « signe via des personnes physiques qui sont signataires »[24]. La notion de signataire – qui selon la vision du ministre se rapproche après analyse de celle de détenteur[25] voire se confond avec cette notion – risquait donc d'entraîner une confusion entre le titulaire et le détenteur des éléments permettant de générer une signature électronique.

Force est toutefois de constater que le terme « signataire » apparaît à de nombreuses reprises dans la loi[26]. Sans doute convient-il de lire ce terme en gardant à l'esprit la définition de titulaire de certificat puisque la loi semble ne pas vouloir s'occuper des détenteurs des données afférentes à la création de signature.

2. Données afférentes à la création et à la vérification de signature (art. 2, 6° et 8°)

L'article 2, 6°, définit les *données afférentes à la création de signature* comme « des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique avancée » et l'article 2, 8°, précise que les *données afférentes à la vérification de signature* sont « des données, telles que des codes ou des clés

[21] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 20.

[22] Le cas échéant, le titulaire sera bien avisé de répercuter ses obligations et responsabilités sur l'éventuel détenteur.

[23] Amendement n° 1 de M. Steverlynck, *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/2, p. 1.

[24] *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, p. 4.

[25] La loi type de la CNUDCI sur les signatures électroniques va dans le même sens. Elle définit en son article 2, point d), le *signataire* comme une « personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente ». La définition du même concept proposée par la directive européenne est plus surprenante car elle vise une personne qui détient, non pas des *données afférentes à la création de signature*, mais un *dispositif de création de signature* (art. 2, point 3) !

[26] C'est notamment le cas dans l'article 2, 2° et 6°, ainsi qu'à l'annexe I, points c), d) et e).

cryptographiques publiques, qui sont utilisées pour vérifier une signature électronique avancée ».

Ces concepts apparaissent relativement abstraits. Ils découlent directement de la directive et permettent de sauvegarder le principe de neutralité technologique. Dans une infrastructure à clé publique, ces deux notions visent respectivement la clé privée (utilisée pour signer) et la clé publique (utilisée par le destinataire du message pour vérifier la signature). Néanmoins, il est probable qu'à l'avenir d'autres technologies, ne reposant pas nécessairement sur l'utilisation de clés asymétriques, répondront aux éléments de ces définitions. Par exemple, dans le contexte des signatures biométriques, l'élément essentiel et unique serait notamment l'empreinte digitale ou les données de balayage de la rétine.

Selon la définition de données afférentes à la création de signature, les codes ou clés utilisés pour créer une signature électronique avancée doivent être uniques. Cette exigence d'unicité impose, nous semble-t-il, que le prestataire de service de certification vérifie que telle clé ou tel code n'a pas déjà été attribué. Certes, il ne peut opérer cette vérification directement sur les données afférentes à la création de signature, qui par définition doivent être conservées confidentielles par le titulaire[27], mais il peut le faire sur ses « jumelles » à savoir les données afférentes à la vérification de signature, qui sont complémentaires aux premières. En pratique, cette vérification ne pose pas de problèmes particuliers pour les données appartenant aux clients du PSC puisqu'il lui suffit de vérifier dans son propre annuaire de certificats. Par contre, la tâche pourrait s'avérer moins aisée pour les données déjà attribuées aux clients de ses nombreux concurrents !

Cette obligation de vérification d'unicité à charge du PSC n'apparaît pas explicitement dans la loi. Tout au plus l'annexe III précise dans son point a) qu'un dispositif de création de signature, pour être qualifié de sécurisé, doit garantir que les « données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois… ». Pour rappel, il est nécessaire d'utiliser un dispositif sécurisé de création de signature pour pouvoir revendiquer les effets de la clause d'assimilation de l'article 4, § 4. Or l'utilisation d'un tel dispositif ne relève pas expressément d'une obligation ou de la responsabilité du PSC qui émet des certificats qualifiés[28] mais bien du titulaire lui-même qui souhaite bénéficier de la clause précitée.

La définition de données afférentes à la vérification de signature permet de rappeler que lors de la réception d'un message signé électroniquement, il est en principe nécessaire d'effectuer systématiquement une opération de vérification de signature afin de vérifier la validité de cette dernière. Nous aurons l'occasion de revenir sur cette problématique.

3. Dispositif (sécurisé) de création de signature et dispositif de vérification de signature (art. 2, 7° et 9°)

L'article 2, 7°, définit le *dispositif sécurisé de création de signature* comme « un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'annexe III de la présente loi » et le *dispositif de*

[27] Voyons à ce propos l'article 19, § 1er, ainsi que le point j) de l'annexe II.

[28] Sauf si le PSC souhaite obtenir une accréditation : il doit alors utiliser des dispositifs sécurisés de création de signature (art. 17, § 1er). Une telle obligation, à charge des PSC qui délivrent des certificats qualifiés sans accréditation, n'est pas expressément consacrée par la loi.

vérification de signature comme « un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature ».

Ces notions n'appellent pas de commentaires particuliers. Selon l'exposé des motifs, elles visent par exemple le logiciel qui permet de générer les données afférentes à la création et à la vérification de signature, celui qui permet de créer et/ou de vérifier une signature électronique[29], la carte à puce sur laquelle sont stockées les données afférentes à la création de signature, le lecteur de carte à puce, etc.[30]

Les dispositifs de création de signature ne sont considérés comme *sécurisés* que s'ils satisfont aux exigences de l'annexe III. Ces dernières sont libellées en termes très généraux : les dispositifs doivent garantir l'unicité et le maintien de la confidentialité[31] des données utilisées pour créer la signature électronique ; l'impossibilité de déduire les données utilisées pour créer la signature à partir de celles utilisées pour vérifier la signature (connues de tous) ; l'impossibilité de falsifier techniquement la signature ; la possibilité pour le « signataire » de protéger techniquement (par un mot de passe ou un contrôle biométrique par exemple) les données utilisées pour créer la signature afin d'empêcher tout accès illégitime à œlles-ci. Enfin, ces dispositifs ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au « signataire » avant le processus de signature. Il apparaît en effet indispensable que le signataire puisse visualiser, vérifier le contenu, repérer d'éventuelles modifications, et ainsi adhérer à ce qu'il signe.

Il n'est pas aisé en pratique de déterminer les dispositifs de création de signature électronique qui satisfont à ces exigences, et qui peuvent ainsi revendiquer le statut de dispositif *sécurisé*. Toutefois, selon l'article 3, point 5, de la directive et l'article 6 de la loi, la Commission attribuera, et publiera au *J.O.C.E.*, des numéros de référence de normes généralement admises pour des produits de signature électronique. L'article 6 précise que lorsqu'un produit de signature électronique, concept qui inclut les dispositifs de création de signature électronique, est conforme à ces normes, celui-ci est **présumé satisfaire** aux exigences de l'annexe III. Pour les dispositifs sécurisés de création de signature électronique, cette présomption de conformité fait l'objet d'une reconnaissance publique puisque l'article 7, § 2, ajoute que « la conformité des dispositifs sécurisés de création de signature électronique par rapport aux exigences visées à l'annexe III de la présente loi est attestée par des organismes compétents désignés par l'Administration …»[32]. Le paragraphe 3 indique qu'il appartient au Roi de déterminer les conditions auxquelles doivent répondre ces organismes. Pour ce faire, le Roi devra impérativement se conformer à la décision de la Commission du 6 novembre 2000 qui fixe les critères minimaux (impartialité, indépendance financière, compétence professionnelle, etc.) à respecter pour la désignation de ces organismes[33]. Espérons que lorsque ces organismes seront désignés, ils œuvreront dans la plus grande transparence et indiqueront clairement au public les dispositifs dont ils attestent la conformité à l'annexe III. En effet, pour rappel, l'utilisation d'un dispositif *sécurisé* de création de signature est une des conditions pour

[29] Il peut s'agir d'un navigateur ou d'un logiciel de courrier électronique, répandu sur le marché, qui intègre les fonctionnalités de signature électronique, ou d'un logiciel propriétaire.
[30] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 21.
[31] L'annexe III tempère cette obligation par la notion du *raisonnable*.
[32] Dans une perspective européenne, l'article 7, § 4, ajoute que la « conformité établie par un organisme désigné par un autre Etat membre de l'Espace économique européen est reconnue en Belgique ».
[33] Décision de la Commission du 6 novembre 2000 relative aux critères minimaux devant être pris en compte par les Etats membres lors de la désignation des organismes visés à l'article 3, paragraphe 4, de la directive 1999/93/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques, 2000/709/CE, *J.O.C.E.*, L 289/42 et 43 du 16 novembre 2000.

pouvoir bénéficier de la clause d'assimilation consacrée par l'article 4, § 4. En attendant, les incertitudes quant à l'application de cette clause subsistent.

4. Certificat – Certificat qualifié (art. 2, 3° et 4°)

La notion de *certificat* est fondamentale dans le contexte de la certification électronique. Selon l'article 2, 3°, il s'agit d'une « attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale et confirme l'identité de cette personne ». Par l'émission du certificat, le prestataire de service de certification « certifie » ce lien et affirme publiquement l'exactitude des informations qu'il contient. Cette définition ne semble pas viser les autres certificats que ceux d'identité, tels que certificats relatifs à un serveur, à un logiciel, à un label voire même les certificats relatifs au temps, dont on déduit qu'ils ne rentrent pas dans le champ d'application de la loi.

Le certificat est élevé au rang des *certificats qualifiés* s'il satisfait aux exigences visées à l'annexe I – c'est-à-dire s'il contient un minimum d'informations – et s'il est fourni par un PSC satisfaisant aux exigences visées à l'annexe II - c'est-à-dire s'il a été émis dans des conditions sûres. Nous aurons l'occasion de commenter le contenu de ces annexes par la suite. Rappelons que pour bénéficier de la clause d'assimilation consacrée par l'article 4, § 4, la signature électronique doit être réalisée sur la base d'un certificat qualifié.

5. Prestataire de service de certification (art. 2, 10°)

Selon l'article 2, 10°, le *prestataire de service de certification* est « toute personne physique ou morale qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques ». Dans la pratique, il s'agira souvent d'une personne morale.

Le champ d'application de cette définition est surprenant. Telle qu'elle est libellée, serait un PSC soumis à l'application de la loi tout prestataire dont la mission principale est la création, la délivrance et la gestion de certificats, fournissant éventuellement des services supplémentaires connexes à l'utilisation des signatures électroniques (horodatage, archivage, enregistrement, annuaire, consultance…) mais également les prestataires qui fourniraient ces derniers services sans toutefois délivrer des certificats ! Ainsi, selon une interprétation stricte de la définition, une autorité d'enregistrement qui se limite à exercer la fonction d'enregistrement[34] – c'est-à-dire une personne physique ou morale dont la seule mission est de collecter de manière fiable les informations destinées à figurer sur le certificat pour ensuite les transmettre au prestataire qui va générer le certificat – pourrait être qualifiée de PSC au sens de la loi !

Cela nous semble excessif et ne correspond pas à la philosophie de la loi dont on constate que l'ensemble des obligations et responsabilités sont liées à la fonction première du PSC à savoir la délivrance de certificats. L'exposé des motifs semble admettre ce partage des fonctions tout en précisant qu'un seul prestataire assume l'entière responsabilité des différentes étapes du processus de certification : « le PSC n'est pas tenu d'assurer seul toutes les étapes du processus de certification. En effet, il peut se référer, pour la collecte des informations, aux renseignements détenus par les autorités d'enregistrement. Toutefois, il répond, à l'égard des utilisateurs des certificats, du dommage qui est la conséquence des obligations qui lui sont

[34] Comme le font ou pourraient le faire certaines agences bancaires, les bureaux de poste, les guichets communaux, les ordres professionnels, les Chambres de Commerce et d'industrie, etc.

imposées par ou en vertu de la présente loi »[35]. Ainsi, si le PSC délivrant des certificats souhaite sous-traiter la tâche d'enregistrement à la société X (art. 8, § 2), celle de vérification de la complémentarité des données afférentes à la création et à la vérification de signature à la société Y (art. 8, § 1er) et enfin celle de conservation d'un annuaire électronique ainsi que celle de procéder à la révocation des certificats à la société Z (art. 10 et 12), il n'empêche que le PSC qui délivre le certificat assume ces différentes obligations et l'éventuelle responsabilité découlant de leur non exécution[36]. L'utilisateur se retrouve donc juridiquement face à un interlocuteur unique : le PSC délivrant le certificat et identifié comme tel dans le certificat qualifié (annexe I, point b).

Pour éviter la confusion, sans doute eut-il été plus judicieux de remplacer dans l'article 2, 10°, le mot « ou » par les mots « et, le cas échéant, ». La loi type de la CNUDCI sur les signatures électroniques est plus précise à cet égard. En son article 2, point f), elle définit le prestataire de service de certification comme une « personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques »[37]. Cette précision aurait permis d'éviter l'ambiguïté tout en indiquant que ce n'est pas parce qu'un PSC offre d'autres services que celui de délivrance et de gestion de certificat qu'il n'est plus un PSC au sens de la loi et soumis à l'application de celle-ci.

6. Produit de signature électronique (art. 2, 11°)

La notion de *produit de signature électronique* est particulièrement ouverte. Elle englobe non seulement les notions de dispositifs de création et de vérification de signature (cf. *supra*) mais également tout autre produit lié à la signature électronique. En effet, selon la directive (considérant n° 9), la définition de ces produits ne doit pas être limitée à la délivrance ou à la gestion de certificats mais doit également couvrir tout autre produit utilisant ou permettant d'utiliser des signatures électroniques ou connexe à celles-ci, tels ceux utilisés pour les services d'enregistrement, les services horodateurs, les services d'annuaires ou autres services informatiques. La définition ne vise toutefois que les produits destinés à être utilisés par les prestataires de service de certification. Il est vrai que les produits destinés à être utilisés par les « signataires » sont déjà englobés dans les notions de dispositifs de création et de vérification de signature.

Il va sans dire que ces produits doivent présenter un niveau acceptable de fiabilité. Fort heureusement, cette fiabilité sera parfois présumée. En effet, l'article 6 indique que « Lorsqu'un produit de signature électronique est conforme à des normes dont les numéros de référence sont publiées au *J.O.C.E.* conformément à la procédure visée par la [directive européenne sur les signatures électroniques], ce produit est présumé conforme aux exigences visées à l'annexe II, point f), et à l'annexe III de la présente loi»[38]. Espérons que la procédure d'adoption et de publication de ces normes aboutira rapidement mais surtout suivra le rythme effréné de l'évolution technologique.

---

[35] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 21.

[36] En ce sens également : « D'une manière générale, le prestataire de service peut, sous sa responsabilité, sous-traiter, une partie de ses missions », *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 20.

[37] Loi type de la CNUDCI sur les signatures électroniques du 5 juillet 2001, disponible sur le site suivant : http://www.un.or.at/uncitral/fr-index.htm

[38] L'article 6 est la seule disposition de la loi qui fait référence à la notion de produit de signature électronique, ce qui réduit assez bien l'intérêt de cette définition.

7. Administration et entité (art. 2, 12° et 13°)

L'*Administration* joue un rôle de première importance. Elle est chargée, d'une part, des tâches relatives à l'accréditation éventuelle d'un prestataire de service de certification (art. 17, §1er, et art. 18), d'autre part, de contrôler les prestataires de service de certification délivrant des certificats qualifiés au public et établis en Belgique (art. 20). Il s'agit d'une administration spécialisée constituée au sein du ministère des Affaires économiques[39].

Dans le cadre de la procédure d'accréditation, l'Administration peut s'adjoindre l'aide d'une *entité* qui évaluera la conformité des PSC et des produits de signature électronique aux exigences des annexes I, II et III (art. 17, § 1er, alinéa 2). Pour pouvoir jouer ce rôle, l'entité doit être un « organisme qui démontre sa compétence sur base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen ». Précisons que les notions de certificat et d'accréditation visées par la loi du 20 juillet 1990 s'éloignent de celles consacrées par la loi du 9 juillet 2001 commentée dans le cadre de cette contribution (cf. *infra*).

B. Champ d'application

L'objectif principal de la loi est de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique ainsi que d'assurer une reconnaissance juridique de celle-ci[40]. Un moyen de créer et de renforcer cette confiance consiste à établir un cadre juridique clair qui détermine les droits et obligations des différents intervenants.

C'est ce qu'exprime l'article 3, alinéa 1, en indiquant que « La présente loi fixe certaines règles relatives au cadre juridique pour les signatures électroniques et définit le régime juridique applicable aux opérations effectuées par les prestataires de service de certification ainsi que les règles à respecter par ces derniers et les titulaires de certificats… ». En vue de prendre en compte la reconnaissance de la signature des personnes morales, les mots « … sans préjudice des dispositions légales concernant les règles de représentations des personnes morales » ont été ajouté par rapport à la première version du projet de loi[41]. Sur ce point, nous renvoyons à la contribution de Bernard Vanbrabant dans le présent ouvrage.

Selon l'alinéa 2 de l'article 3, « La présente loi instaure également un régime d'accréditation volontaire ». D'après l'exposé des motifs, cet alinéa aurait été ajouté afin de préciser qu'il s'agit d'une accréditation différente de celle prévue par la loi du 20 juillet 1990. En sus, cet alinéa permet de consacrer le principe de la directive selon lequel les Etats membres ne peuvent soumettre la fourniture de services de certification à aucune autorisation préalable[42].

Nous conviendrons que l'article 3 ne crée pas de droits et d'obligations. Pour partie, il aurait pu trouver sa place dans l'exposé des motifs. Certains parlementaires avaient d'ailleurs

[39] A ce sujet, des informations sont disponibles à l'adresse suivante : http://www.mineco.fgov.be/information_society/index_fr.htm
[40] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 10.
[41] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 19.
[42] Article 3, point 1, de la directive européenne sur les signatures électroniques.

proposé de le supprimer[43]. Malgré le peu de commentaires suscités par cet article, nous relevons toutefois deux modifications mineures par rapport à la version originaire du projet de loi[44] qu'il convient de mettre en avant.

Premièrement, les mots « utilisateurs de certificats » ont été remplacés par les mots « titulaires de certificats ». En effet, lors des discussions parlementaires, on a relevé que la notion « d'utilisateurs de certificats » n'était définie ni dans le projet de loi ni dans la directive, ce qui amena le ministre à considérer qu'il s'agissait en fait des « titulaires de certificats » tels que définit à l'article 2, 5°[45].

Nous regrettons la disparition des mots « utilisateurs de certificats » qui avaient leur raison d'être. En effet, dans la première mouture du projet, des obligations pesaient tant sur le titulaire de certificat – la personne qui signe le message – que sur le destinataire de message – la personne qui reçoit le message signé électroniquement –, dont notamment l'obligation de vérifier la signature et la non révocation du certificat. La notion d'utilisateur de certificat permettait d'englober ces deux catégories de personnes[46]. Force est de constater que les obligations à charge du destinataire du message ont mystérieusement disparu du texte adopté. Faut-il en déduire que le destinataire de message n'est soumis à aucune obligation ? Nous ne le croyons pas. Nous reviendrons par la suite sur cette question.

Deuxièmement, l'ancien paragraphe 2 selon lequel « La présente loi s'applique aux prestataires de service de certification exerçant leurs activités en réseaux ouverts » a été supprimé. Nous approuvons cette suppression notamment parce que la notion de réseau ouvert n'était pas définie et que la distinction réseau ouvert – réseau fermé peut prêter à confusion[47]. Pour nous éclairer sur cette distinction, tout au plus le considérant n° 16 de la directive européenne donne quelques indications en précisant qu'on est en présence d'un réseau fermé lorsque « les signatures électroniques sont utilisées exclusivement à l'intérieur de systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants ». Par ailleurs, le maintien de ce paragraphe risquait d'être interprété comme privant tout prestataire agissant en réseau fermé du droit de demander une accréditation, ce qui ne correspond pas à l'objectif poursuivi par la loi[48].

Cette suppression n'est pas de nature à porter préjudice aux nombreuses conventions utilisées dans la pratique (accords EDI, conventions bancaires, etc.) par lesquelles les parties acceptent l'usage de l'une ou l'autre technique de signature électronique et lui reconnaissent les mêmes effets juridiques que ceux reconnus à la signature manuscrite, encore même la technique visée conventionnellement ne répondrait pas à l'ensemble des conditions pour pouvoir bénéficier de la clause d'assimilation établie par la loi. Il est vrai que cette dernière trouve essentiellement

[43] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/3, p. 9 ; Amendement n° 2 de M. Steverlynck, *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, pp. 4-5.

[44] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 68-81.

[45] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/3, p. 9.

[46] Le commentaire de l'article 3 du projet de loi déposé le 16 décembre 1999 ne peut être plus clair : « On entend par utilisateurs de certificats aussi bien les titulaires de certificats créés et délivrés par un prestataire de service de certification que les destinataires de messages signés électroniquement », *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 22. Voy. aussi les articles 20 et 21 du projet de loi à la page 80 de ces mêmes documents parlementaires.

[47] Pour s'en convaincre, il suffit d'analyser l'interprétation qui en est faite par la Commission européenne dans son avis circonstancié tel que relaté dans l'exposé des motifs : *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 19.

[48] En ce sens, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 19.

son utilité en « réseaux ouverts », dans lesquels les parties ne peuvent régler préalablement les questions de preuve par voie conventionnelle. Pour le reste, le caractère supplétif des règles de preuve, unanimement reconnu par la jurisprudence[49], n'est pas mis à mal.

Si la validité des conventions relatives à la preuve n'est pas remise en cause, se pose néanmoins la question du caractère impératif des dispositions de la loi, spécialement lorsque le PSC délivre des certificats qualifiés. La suppression du paragraphe selon lequel la loi ne s'applique qu'aux PSC qui exercent leurs activités en réseaux ouverts laisse supposer qu'il n'est pas possible de déroger aux dispositions de la loi alors que le considérant n° 16 de la directive indique clairement que « un cadre réglementaire n'est pas nécessaire pour les signatures électroniques utilisées exclusivement » en réseaux fermés tels que définis par cette directive. Il nous semble que l'on devrait pouvoir régler le problème en apportant une nuance à la notion de réseau fermé, et plus exactement en distinguant réseau fermé *au sens strict* et réseau fermé *au sens large*. Ainsi, serait un réseau fermé au sens strict tout réseau qui présente deux éléments : il existe des accords volontaires entre participants mais en plus le nombre de participants est clairement défini[50]. En d'autres mots, ce réseau n'a pas pour vocation de s'étendre dans le cadre d'une logique commerciale sous-jacente[51]. A l'inverse, serait un réseau fermé au sens large, un réseau dans lequel il existe des accords volontaires entre participants[52] mais dont le nombre n'est pas défini mais peut varier, notamment à la hausse, en fonction de la politique commerciale menée par la personne qui gère le réseau, en l'occurrence le PSC. Pour le dire autrement et pour reprendre les termes de la loi, ce serait le cas lorsque le PSC délivre des certificats (qualifiés ou non) « à l'intention du public » ou « au public » (art. 14, 16 et 20, § 2) alors même que tous les participants accepteraient une convention préalable.

Cette distinction réseau fermé au sens strict-large étant faite, il est raisonnable de permettre aux PSC qui délivrent des certificats, encore même seraient-ils qualifiés, dans le cadre d'un réseau fermé au sens strict de pouvoir déroger aux dispositions de la loi, y compris aux règles de responsabilité[53]. Le considérant n° 16 précité abonde dans ce sens. Par contre, si le prestataire exerce ses activités en réseau fermé au sens large – qui ne rentre pas précisément dans la notion du considérant n° 16 –, il est soumis au régime juridique consacré par la loi dès lors que celui-ci délivre des certificats *qualifiés*, voire obtient une accréditation. Cette réflexion revient à consacrer le caractère impératif des dispositions de la loi lorsqu'un PSC exerce ses activités en réseaux ouverts ou en réseaux fermés au sens large. Dans ce cadre, un PSC qui délivre des certificats *qualifiés* pourrait difficilement prétendre être dispensé des exigences de la loi (obligation de respecter les exigences de l'annexe II, de révoquer immédiatement le certificat, de conserver un annuaire électronique…) ou se soustraire au régime de responsabilité, au seul motif qu'il « fermerait » le réseau par conventions !

---

[49] Selon la Cour de cassation, les dispositions légales relatives à la preuve ne sont ni d'ordre public (Cass., 30 janv. 1947, *Pas.*, 1947, I, p. 29 ; 30 sept. 1948, *Pas.*, 1948, I, p. 520 ; 20 juin 1957, *Pas.*, 1957, I, p. 1256) ni impératives (Cass., 16 oct. 1962, *Pas.*, 1963, I, p. 229 ; 22 mars 1973, *Pas.*, 1973, I, p. 695 ; 24 juin 1994, *Pas.*, 1994, I, p. 651).

[50] Cette notion répond à la définition proposée par le considérant de la directive.

[51] Ce serait le cas d'un réseau interne d'une entreprise ou d'un réseau d'entreprises ayant des relations d'affaires stables et régulières.

[52] Notamment, des contrats d'adhésion proposés par le PSC, qui chapeaute et gère le réseau, à ses clients, ces derniers étant à la fois des titulaires et des personnes qui se fient aux certificats en tant que destinataires de messages.

[53] Sous réserve toutefois des limites jurisprudentielles classiques (cf. *infra*).

Dans cette optique, si un PSC qui délivre des certificats dans le cadre d'un réseau fermé *au sens large* souhaitait échapper aux obligations de la loi, et notamment au régime de responsabilité mis en place par celle-ci, il lui suffirait de ne pas indiquer dans les certificats qu'il émet la mention « certificat *qualifié* ». Notons toutefois que cette opportunité devrait, selon nous, être utilisée avec modération. En effet, un juge pourrait estimer que certaines obligations de la loi (obligation de vérifier adéquatement l'identité du demandeur du certificat, de révoquer immédiatement le certificat suite à une demande de son titulaire, de conserver un annuaire électronique accessible en permanence, de prendre des mesures contre la contrefaçon des certificats…) sont considérées comme des obligations essentielles, encore même les certificats émis ne seraient-ils pas réputés *qualifiés*. Or, on sait qu'il n'est pas possible d'écarter conventionnellement toute responsabilité en cas d'inexécution de telles obligations.

C. Principes généraux

La loi consacre trois principes fondamentaux dont il convient de préciser la portée : le principe du libre choix du mode de signature par l'utilisateur (art. 4, § 1) ainsi que celui de recourir à un PSC accrédité (art. 17, § 3), d'une part, et le principe de liberté d'accès au marché pour les PSC, d'autre part (art. 4, § 2).

Libre choix du mode de passation des actes juridiques – Selon le premier paragraphe de l'article 4, « A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique ». Toute personne conserve en principe le libre choix du support – papier ou électronique – par lequel il pose ses actes juridiques. Il nous paraît utile de préciser la portée de cette disposition.

Ce principe de liberté s'applique-t-il également aux personnes morales ? La formulation générale de la disposition plaide en faveur d'une réponse affirmative à cette question. Si le législateur avait voulu réserver le bénéfice de ce droit aux seules personnes physiques, il aurait dû limiter son champ d'application. Il en résulte qu'aucune norme hiérarchiquement inférieur à une loi ne peut imposer à une personne, qu'elle soit physique ou morale, de poser un acte juridique sous forme électronique.

Une autre précision sur la portée de la disposition du paragraphe premier doit également être formulée. En effet, on s'est inquiété du risque que celle-ci soit invoquée en vue de remettre en cause la validité des nombreuses conventions qui imposent l'utilisation de moyens électroniques de signature voire de faire obstacle aux sites de commerce électronique sur lesquels tous les actes juridiques posés le sont nécessairement par voie électronique, et pourquoi pas faire obstacle à l'ensemble des moyens de paiement électronique ! Notons d'emblée que nous ne pensons pas qu'il s'agit là d'hypothèses de *contrainte* telle que visée par l'article 4, § 1er, mais bien de conventions librement consenties entre parties ou d'actes juridiques posés, certes par voie électronique, mais volontairement par l'internaute qui utilise le site de commerce électronique ou le moyen de paiement.

Lors des discussions parlementaires, le ministre a catégoriquement écarté ce risque en soulignant que « la disposition du paragraphe 1er ne concerne pas les relations entre particuliers mais bien les relations des particuliers avec les autorités. Il est évident que des personnes morales privées et des personnes physiques sont libres de prévoir que des actes

juridiques peuvent avoir lieu entre elles par voie électronique »[54]. De la sorte, le ministre réaffirme le principe de l'autonomie de la volonté et le caractère supplétif des règles de preuve. Afin de préciser la portée de la disposition, un Sénateur a proposé l'amendement suivant : « A défaut de dispositions légales contraires, nul ne peut être contraint, dans ses rapports avec les autorités publiques, de poser un acte juridique par voie électronique »[55]. Cet amendement n'a malheureusement pas été adopté. C'est pourtant dans ce sens que l'article 4, § 1, doit être interprété.

La formulation du premier paragraphe de l'article 4 ne limite pas à préciser que toute personne doit garder le libre choix d'utiliser la signature manuscrite ou de recourir à une signature électronique pour formaliser son engagement juridique. En effet, contrairement à la première version du projet de loi qui indiquait que « nul ne peut être contraint de signer électroniquement »[56], la nouvelle formulation est différente en visant le principe de la *passation d'un acte juridique par voie électronique*, peu importe que ce dernier soit signé électroniquement ou non.

Relevons que l'interdiction d'imposer à une personne d'agir par voie électronique ne couvre en principe que la création d'actes juridiques. Qu'en est-il des nombreuses démarches que le citoyen ou l'entreprise doit accomplir vis-à-vis de l'administration ? Ces communications avec l'administration sont-elles visées par l'interdiction ? En théorie, si la communication peut s'analyser en un acte juridique, c'est-à-dire en une émission de la volonté en vue de créer des droits et des obligations, l'interdiction joue. Dans le cas contraire, l'interdiction ne pourrait être soulevée et une personne pourrait être contrainte d'effectuer les démarches administratives par voie électronique même en l'absence d'une loi ! En pratique toutefois, cette interprétation semble délicate non seulement parce que la qualification d'une démarche administrative en un acte juridique est une opération acrobatique et peu commune mais aussi parce qu'elle ne correspond pas à la volonté du législateur qui entend conjurer le risque de réduire les possibilités d'accès à l'administration, et d'augmenter ainsi les inégalités entre les citoyens, qui découlerait de l'obligation de s'adresser à elle exclusivement par voie électronique. C'est donc probablement toutes les démarches avec les autorités, quelles qu'elles soient, qui sont visées par la disposition[57]. Dans cette optique, utiliser le terme « acte juridique » n'était probablement pas le plus adéquat !

Libre choix de recourir à un PSC accrédité ou non – Le deuxième principe général qui intéresse les utilisateurs de signatures électroniques est consacré par l'article 17, § 3, selon lequel, « Le choix de recourir à un prestataire de service de certification accrédité est libre ». La loi met en place un système volontaire d'accréditation (cf. *infra*) qui permet la coexistence sur le marché de PSC accrédités et de PSC non accrédités. Dans ce contexte, la personne qui décide d'utiliser une signature électronique doit rester libre de se faire délivrer un certificat par l'un ou l'autre de ces prestataires[58], et si elle opte pour un PSC accrédité, elle doit rester libre de son choix parmi les différents PSC accrédités. A l'instar de l'article 4, § 1er, la porté de cette disposition prête à discussion.

---

[54] *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, p. 5.
[55] *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/2, p. 5.
[56] Article 4, § 2, du projet de loi du 16 décembre 1999, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 23 et 70.
[57] Les travaux préparatoires précisent d'ailleurs que la disposition du § 1er concerne les relations avec les autorités, *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, p. 5.
[58] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 23.

La disposition a pour vocation, à tout le moins, d'éviter que des dispositions réglementaires viennent exiger systématiquement l'utilisation des services offerts par des PSC accrédités, ce qui aurait pour effet de ruiner le principe de non autorisation préalable[59] en créant indirectement un système d'accréditation obligatoire[60]. A défaut de disposition légale contraire, il n'est en principe pas possible d'exiger qu'un utilisateur soit titulaire d'un certificat émis par un PSC accrédité.

Un tempérament pourrait néanmoins être apporté à ce principe. En effet, l'article 4, § 3, stipule que « Le Roi peut, par arrêté délibéré en Conseil des Ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles ». Dans ce cadre, on pourrait imaginer l'adoption d'un arrêté royal, justifié par le fait que certaines applications dans le secteur public exigent un niveau de sécurité supérieur, qui imposerait le recours à des PSC accrédités. Si cette interprétation venait à être autorisée, l'utilisation de cette prérogative serait toutefois soumise au respect de plusieurs conditions. Premièrement, l'arrêté doit être délibéré en Conseil des Ministres. Deuxièmement, cette prérogative ne peut être exercée que pour des applications dans le secteur public et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée : un tel arrêté royal ne peut être pris dans le cadre des relations avec les consommateurs ou ne peut prévoir de manière générale que, dans toutes ses relations avec une autorité publique, le citoyen est tenu d'utiliser un certificat émis par un PSC accrédité. Troisièmement, les exigences supplémentaires (en l'occurrence, le recours à un PSC accrédité) ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens.

Qu'en est-il de l'application de l'article 17, § 3, dans les relations entre partenaires privés ? Cet article fait-il obstacle par exemple à ce qu'un responsable d'un site de commerce électronique exige que les internautes qui souhaitent passer une transaction sur le site soient titulaires d'un certificat émis par un PSC accrédité ? Les travaux parlementaires sont muets sur ce point. Il semble qu'une telle hypothèse ne porte pas atteinte à l'article 17, § 3 : le fait que certains site web exigent d'être en possession d'un certificat émis par un PSC accrédité n'entrave pas le choix de l'utilisateur potentiel de recourir à un PSC accrédité ou non. Tout au plus, les utilisateurs qui sont clients d'un PSC non accrédité ne pourront effectuer de transactions sur les sites web en question. La situation n'est guère différente de celle des personnes qui ne sont pas titulaires d'une carte de crédit et qui ne peuvent, de ce fait, effectuer de transactions sur la plupart des sites web de commerce électronique. Il convient toutefois de veiller à ce que cet état de fait ne soit pas de nature à fausser les règles de concurrence.

Principe de liberté d'accès au marché – Le troisième principe général intéresse les prestataires de service de certification. Conformément à l'article 3 de la directive européenne qui vise notamment à assurer la liberté de fourniture des services de certification, l'article 4, § 2, de la loi consacre le principe de non autorisation préalable. Cela signifie qu'un prestataire de service de certification n'a pas l'obligation de demander une autorisation préalable – en l'occurrence une accréditation ou toute autre mesure ayant un effet équivalent – pour exercer ses activités. Si un régime d'accréditation est mis en place (cf. *infra*), celui-ci doit nécessairement rester volontaire.

[59] Article 3.1. de la directive ; article 4, § 2, de la loi.

[60] En effet, les PSC pourraient être dans les faits contraints à demander une accréditation en constatant que l'absence de cette dernière leur empêche de toucher la majorité des clients potentiels et donc de gagner des parts de marché.

Il convient néanmoins de préciser que la loi soumet les PSC accrédités, et plus généralement les PSC délivrant des certificats qualifiés établis en Belgique, à une déclaration préalable. En effet, l'article 4, § 2, alinéa 2, oblige ces derniers à communiquer à l'Administration avant le début de leurs activités leurs coordonnées, leurs références ainsi que la preuve qu'une assurance a été souscrite en vue de couvrir leurs obligations en matière de responsabilité[61]. Cette obligation, qui rappelons-le ne pèse que sur les PSC délivrant des certificats qualifiés établis en Belgique et qui ne s'apparente pas à une autorisation préalable, vise notamment à permettre à l'Administration d'exercer son pouvoir de contrôle consacré par l'article 20.

Rappelons que l'article 4, § 3, permet au Roi de soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Le cas échéant, il pourrait par exemple exiger que l'utilisateur se présente auprès d'un guichet communal pour effectuer sa demande de certificat et s'identifier, indique obligatoirement le numéro d'identification social sur les certificats qualifiés utilisés pour les applications avec les administrations sociales, obtienne un certificat auprès d'un PSC accrédité[62], lui même soumis à des exigences de sécurité spécifiques, etc. Signalons également que pour ce faire, l'arrêté fixant les exigences supplémentaires doit être délibéré en Conseil des Ministres, les exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée et, enfin, ces exigences ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens.

Section 3.
Le régime juridique des PSC

On a vu que le rôle du prestataire de service de certification dans la société de l'information, et notamment dans une infrastructure à clé publique, est à ce point capital qu'il a justifié l'adoption d'un régime juridique précis et unifié. Hormis celles relatives à la protection de la vie privée, les règles s'appliquent exclusivement aux PSC délivrant des certificats qualifiés.

A. Tronc commun applicable à l'ensemble des PSC : la protection de la vie privée

Que le PSC délivre des certificats qui sont qualifiés ou non, il est tenu de respecter les exigences de l'article 5, qui traite de la protection de la vie privée[63]. Ce texte constitue une transposition fidèle de l'article 8 de la directive européenne. Il commence par rappeler que les règles du droit commun de la vie privée consacrées par la loi du 8 décembre 1992[64] sont pleinement applicables. En effet, pour pouvoir établir un certificat, le PSC doit être en mesure de vérifier de manière certaine et non équivoque l'identité du candidat titulaire. A cette fin, il

[61] Si le PSC qui délivre des certificats qualifiés n'exécute pas cette obligation de déclaration préalable, il pourra se voir appliquer les sanctions prévues à l'article 20 (cf. *infra*).

[62] Dans ce cas, l'avenir nous apprendra si la Commission européenne accepte une telle exigence, dont elle peut estimer qu'elle a pour effet de créer, indirectement, un système d'autorisation préalable, explicitement interdit par la directive !

[63] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 20.

[64] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, modifiée par la loi du 11 décembre 1998, *M.B.*, 3 févr. 1999.

est amené à collecter et à conserver diverses données à caractère personnel sur les candidats[65], ce qui justifie l'application de cette loi générale.

L'article 5 semble imposer des contraintes supplémentaires aux PSC qui délivrent des certificats à *l'intention du public*[66]. En effet, ces derniers ne peuvent recueillir des données personnelles, sans le consentement explicite de la personne concernée[67], que *directement* auprès de celle-ci et *uniquement* dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Il en résulte que si le PSC recueille les données autrement que directement auprès de la personne concernée – par exemple en consultant un registre *ad hoc* tel que le registre national ou en obtenant les données d'un tiers, tel que l'employeur qui effectue une demande de certificats pour ses employés –, le PSC doit en principe obtenir le consentement explicite de la personne concernée[68]. Par ailleurs, si le PSC recueille d'autres données personnelles que celles qui sont nécessaires à la délivrance et à la conservation du certificat[69] – telles que par exemple des attributs éventuels que le candidat ne demande pas à faire figurer dans le certificat (les différentes fonctions ou titres honorifiques de la personne concernée, son numéro d'identification sociale, les activités qu'elle exerce habituellement, etc.) –, il doit également obtenir le consentement explicite de la personne intéressée. Il en est de même si le PSC, au delà de la collecte, traite ces données à d'autres fins que la délivrance et la conservation du certificat. Ce serait notamment le cas si le PSC dressait un profil du titulaire sur la base des attributs qui lui ont été communiqués pour lui fournir d'autres services ou s'il transmettait ces données à des tiers.

L'article 5, § 2, donne le droit au titulaire d'obtenir un certificat avec un pseudonyme au lieu de son identité. Cette possibilité était imposée par l'article 8, point 3, de la directive européenne. Ce droit à l'anonymat est toutefois soumis au respect de deux conditions. D'une part, l'annexe I, point c), indique que le pseudonyme doit être identifié comme tel. Notons que l'annexe I ne concerne que les certificats qualifiés. Si le certificat n'est pas qualifié, le PSC n'a en principe pas l'obligation d'indiquer la mention « pseudonyme »[70]. D'autre part, le PSC est tenu de demander et de conserver l'identité réelle du titulaire afin de pouvoir répondre à l'obligation de l'article 5, § 2, selon laquelle, lorsque les nécessités de l'instruction l'exigent, le PSC est tenu de communiquer aux autorités judiciaires toute donnée relative à l'identité du titulaire. Le cas échéant, il n'est tenu de le faire que dans les circonstances et selon les conditions prévues par les articles 90*ter* à 90*decies* du Code d'instruction criminelle relatifs aux écoutes, à la prise de connaissance et à l'enregistrement de communications et de

[65] Le PSC doit par exemple collecter les coordonnées et les éventuels attributs des titulaires (art. 8, § 2), tenir un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat (art. 8, § 3), conserver un annuaire électronique de certificat (art. 10), conserver toutes les informations pertinentes concernant un certificat qualifié pendant 30 ans (annexe II, point i), etc.

[66] On en déduit que ces contraintes supplémentaires ne s'appliquent pas au PSC qui ne délivre pas des certificats à l'intention du public, tel qu'un PSC agissant dans le cadre d'un intranet d'une entreprise et qui délivre uniquement des certificats aux membres de l'entreprise.

[67] C'est-à-dire la personne qui effectue la demande d'un certificat établit à son nom.

[68] Notons toutefois que si l'employeur – personne morale – demande un certificat à son nom, le PSC est tenu en vertu de l'article 8, § 3, de tenir un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat. Dans cette hypothèse, le PSC n'est, selon nous, pas tenu de demander et d'obtenir le consentement explicite de la personne physique en question.

[69] Encore faudra-t-il déterminer les données qui ne sont pas nécessaires à la délivrance et à la conservation du certificat !

[70] Voy. toutefois le point f) de l'annexe IV applicable en principe à tout type de signature et de certificat mais ne constituant que des recommandations.

télécommunications privées. Cette obligation de conservation de l'identité du titulaire pèse sur tous les PSC, même s'ils ne délivrent pas de certificats qualifiés.

B. Les PSC délivrant des certificats qualifiés

Les article 8 à 18 de la loi ne trouvent à s'appliquer qu'aux PSC qui délivrent des certificats *qualifiés* (cf. *supra*). Rappelons qu'il n'est pas nécessaire d'obtenir une accréditation pour émettre ce type de certificats. Dès lors que le PSC délivre des certificats qualifiés, il est tenu de respecter les dispositions des articles 8 à 18 de la loi. Nous commençons par présenter le tronc commun de règles s'adressant à l'ensemble des PSC délivrant des certificats qualifiés (art. 8 à 16), qu'il soient accrédités ou non, pour ensuite commenter les mesures spécifiques aux PSC accrédités (art. 17 et 18).

1. Tronc commun

Au risque d'essuyer les remontrances de l'Administration, le PSC qui, d'initiative, souhaite émettre des certificats qualifiés doit être attentif à l'étendue des missions qui lui sont imparties, respecter les nombreuses exigences relatives aux certificats qualifiés, assumer les responsabilités liées aux spécificités de son activité, le cas échéant opérer la révocation des certificats dans les limites tracées par la loi et, enfin, ne peut mettre fin à ses activités sans avoir accompli certaines démarches préalables.

a) Les missions (art. 8 à 10)

Les articles 8 à 10 de la loi traitent exclusivement des obligations du PSC dans le cadre de sa mission première que constitue la délivrance et la conservation des certificats qualifiés. Ces dispositions ne disent rien des autres missions éventuelles exercées par le PSC (horodatage, archivage, conseil, création d'outils de génération de factures électroniques, etc.), sauf si des certificats qualifiés sont émis dans le cadre de ces autres services.

Vérification de la complémentarité des données – Préalablement à la délivrance du certificat, le PSC est tenu de vérifier la complémentarité des données afférentes à la création et à la vérification de signature (art. 8, § 1er). Cette obligation est logique : dans la mesure où le certificat établit un lien entre l'identité du signataire et les données utilisées pour vérifier la signature, il est primordial de vérifier au début du processus de certification que ces dernières sont mathématiquement appariées aux données qui seront utilisées par ce même signataire pour créer la signature. En l'absence d'une telle vérification, un utilisateur risquerait de faire certifier des données pour lesquelles, sans le savoir, il ne détient pas les données complémentaires de création de signature alors qu'un tiers indélicat les détiendrait peut être… Par ailleurs, le titulaire pourrait reprocher au PSC par la suite que le certificat délivré ne permet pas de vérifier les signatures électroniques qu'il génère. Enfin, indiquons déjà que l'article 14, § 1er, point b), prévoit une présomption de responsabilité à charge du PSC dans l'hypothèse où il ne vérifie pas, au moment de la délivrance du certificat, que le titulaire détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature destinées à figurer dans le certificat. Rappelons toutefois qu'il ne semble pas que la loi impose au PSC de vérifier l'unicité de ces données. Tout au plus, l'assurance de cette unicité découle de l'utilisation d'un dispositif sécurisé de création de signature (cf. *supra*). En tous les cas, lors de la vérification de la complémentarité

des données, le PSC doit s'abstenir de stocker ou copier les données afférentes à la création de signature (annexe II, point j).

L'obligation consacrée par l'article 8, § 1er, ne semble pas faire de distinction selon que le PSC a généré lui même les données ou que celles-ci ont été communiquées par le demandeur du certificat : dans les deux cas, le PSC doit effectuer la vérification[71]. Notons toutefois que l'article 14, § 1er, point c), relatif à la responsabilité du PSC paraît n'envisager que l'hypothèse dans laquelle le PSC génère lui même les deux types de données[72]. Cette limitation dans le texte de l'article 14 n'est de toute évidence pas de nature à exclure toute responsabilité du PSC dans le cas où ce dernier n'opère pas la vérification pour les données générées par le titulaire (cf. *infra*). La disposition de l'article 8, § 1er, s'analyse, nous semble-t-il, en une obligation de résultat « allégée », dont la simple constatation de l'inexécution crée une présomption de responsabilité dans le chef du PSC. Néanmoins, ce dernier peut se dégager de sa responsabilité en apportant la preuve qu'il n'a commis aucune négligence[73] (art. 14, § 1er, *in fine*).

Délivrance du certificat et vérifications préalables – « Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de service de certification délivre un ou plusieurs certificats à toute personne qui en fait la demande » (art. 8, § 2). Ce paragraphe consacre plusieurs obligations à charge du PSC.

Avant tout, le PSC est tenu de vérifier l'identité de la personne, qu'elle soit physique ou morale, qui fait la demande du certificat et, éventuellement, les qualité spécifiques que cette personne souhaiterait faire certifier (un titre, une fonction, un pouvoir, un numéro de TVA…). Si le paragraphe 2 est clair quant à l'existence de l'obligation, il ne souffle mot sur les modalités d'exercice de celle-ci. Pourtant l'enjeu est de taille, puisque le PSC est présumé responsable de l'éventuelle inexactitude des informations contenues dans le certificat, sauf s'il prouve qu'il n'a commis aucune négligence (art. 14, § 1er, point a). Dans ce contexte, des informations complémentaires quant à la manière de satisfaire à l'obligation du paragraphe 2 devraient permettre d'apprécier l'absence éventuelle de négligence dans le chef du PSC, et de le libérer ainsi de sa responsabilité. Néanmoins, la loi est peu loquace à cet égard. Tout au plus, l'annexe II, point d), parle de « moyens appropriés et conformes au droit national ». L'exposé des motifs nous donne quelques éléments supplémentaires de réflexion sur ce point.

Selon l'exposé des motifs, la vérification de l'identité et des qualités spécifiques « doit se faire par des moyens appropriés : cela implique que le prestataire se base sur un document difficilement falsifiable ou sur le recoupement de différents documents. Il peut pour ce faire

[71] Cette obligation est fondamentale et doit, selon nous, peser sur tout PSC qui offre au public des certificats qualifiés, peu importe que les données offertes à la certification aient été générés par le PSC ou par un tiers. En effet, en émettant un certificat, le prestataire confirme le lien entre une personne et ses données afférentes à la vérification de signature. La certification demeure vide de sens si, certifiant ce lien, le PSC omet de vérifier la complémentarité des données. Le cas échéant, cela reviendrait à dire que le PSC certifierait que telles données afférentes à la vérification de signature appartiennent à telle personne mais sans être certain que ces données sont liées *mathématiquement* aux données afférentes à la création de signature.

[72] A cet égard, nous relevons une contradiction entre le point c) et le point a) de l'article 14, § 1er. En effet, le point a) crée une présomption de responsabilité à charge du PSC quant à l'exactitude de toutes les informations contenues dans le certificat qualifié. Or l'annexe I relative aux informations contenues dans le certificat précise dans son point e), que les données afférentes à la vérification de signature doivent correspondrent aux données pour la création de signature, sans faire de distinction si ces données sont générées par le PSC ou par l'utilisateur. On en déduit indirectement une obligation pour le PSC d'effectuer cette vérification, et une responsabilité sous-jacente qui découle du point a) de l'article 14.

[73] On n'exigerait pas qu'il doive se prévaloir d'une cause étrangère libératoire.

s'adjoindre l'aide d'autorités d'enregistrement (communes, La Poste, chambres de commerce, ordres professionnels, etc.). Si le certificat est délivré à une personne morale, le prestataire vérifie préalablement l'identité de la personne morale comme prévu ci-dessus mais aussi l'identité et le pouvoir de représentation de la (ou des) personne(s) physique(s) qui se présente(nt) à lui » [74]. Si la loi exige de s'appuyer sur des documents suffisamment probants pour vérifier l'identité et les qualité spécifiques des personnes (carte d'identité, passeport, certificat de résidence, statuts, attestation d'un ordre professionnel…), elle ne semble pas imposer la comparution personnelle du demandeur auprès du PSC, ou de l'éventuelle autorité d'enregistrement. La demande d'un certificat devrait pouvoir se faire à distance, moyennant l'envoi par La Poste des documents probants, ou par l'intermédiaire d'une autre personne ayant reçu procuration. Il appartient donc à chaque PSC de juger de l'opportunité ou de la nécessité d'un « face-to-face » avant toute délivrance d'un certificat. Le PSC qui considère cette formalité inutile ou trop contraignante doit néanmoins garder à l'esprit qu'il pourrait rencontrer plus de difficultés à apporter la preuve qu'il n'a commis aucune négligence dans l'hypothèse où sa responsabilité serait engagée dans le cadre de l'article 14, § 1er, point a). Il convient en plus de préciser que si la loi du 9 juillet 2001 n'exige pas expressément la présentation physique du candidat titulaire, cela ne supprime pas l'obligation pour le PSC de procéder à cette identification physique dans l'hypothèse où elle serait imposée par d'autres lois[75].

Ensuite, dès lors que le PSC a pu vérifier la véracité des informations destinées à figurer dans le certificat, il est tenu de délivrer le ou les certificats demandés et ne peut en principe pas refuser de manière discrétionnaire cette délivrance[76]. La formulation de l'article 8, § 2, est relativement claire à cet égard. En revanche, cette « obligation de délivrance est levée lorsque le PSC a de sérieux doutes quant à l'identité ou/et une qualité spécifique de la personne physique ou morale et qu'il ne peut le vérifier par des moyens raisonnables »[77]. Par ailleurs, une fois le certificat délivré, le PSC peut de sa propre initiative révoquer le certificat s'il a des doutes sérieux sur la véracité des informations transmises lors de l'enregistrement (art. 12, § 2, 1°).

Enfin, l'article 8, § 2, confirme sans équivoque qu'une même personne peut être titulaire de plusieurs certificats. On peut en effet imaginer qu'une personne physique souhaite obtenir un certificat sans qualité spécifique (certificat citoyen) ainsi que divers certificats avec des qualités spécifiques différentes liées à ses activités professionnelles ou à des applications particulières. Quant aux personnes morales, il est à prévoir que celles-ci demanderont autant de certificats que le nombre de délégations de pouvoir à effectuer au sein de l'entreprise.

Rappelons que d'une manière générale, le PSC peut, sous sa responsabilité, sous-traiter l'une ou l'autre des missions décrites ci-dessus[78].

---

[74] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 28. Sur ce point, nous renvoyons le lecteur à la contribution de Bernard Vanbrabant dans le présent ouvrage.

[75] Nous pensons par exemple à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux, modifiée par la loi du 10 août 1998, *M.B.*, 15 octobre 1998. Pour un commentaire relatif à l'application de cette obligation contraignante sur les réseaux, voy. L. ROLIN JACQUEMYNS et T. VERBIEST, « L'offre de services et produits financiers sur internet », *R.D.C.*, n° 2000/2, pp. 76 et s.

[76] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 28.

[77] *Ibidem*.

[78] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 20.

Tenue d'un registre des « détenteurs » en cas de délivrance de certificats à une personne morale – L'article 8, § 3, quant à lui, impose au PSC qui délivre des certificats qualifiés à des personnes morales de tenir « un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique ». Nous laissons le soin à Bernard Vanbrabant de commenter la portée et l'utilité de cette disposition dans le cadre de sa contribution dans le présent ouvrage. Nous nous interrogeons sur l'opportunité d'une telle obligation, à tout le moins à charge du PSC. On peut éventuellement l'admettre si elle se limite à imposer au PSC de jouer le rôle de dépositaire d'une liste préparée par la personne morale qui fait la demande des certificats et pour laquelle le PSC n'assume aucun contrôle quant au contenu. Par contre, en raison de la charge de travail et des responsabilités que cela implique, on peut difficilement accepter que le PSC soit, au-delà de la simple conservation du registre, tenu de vérifier *in casu* que la personne physique qui fait usage de la signature correspond à celle indiquée dans le registre ainsi que de veiller à la mise à jour de ce registre. Nous pensons que ces tâches relèvent de la responsabilité de la personne morale elle même.

Fourniture d'un exemplaire du certificat – Une fois le certificat généré, l'article 9 impose au PSC de fournir un exemplaire de ce dernier au candidat titulaire. Le libellé de cet article nous laisse songeur. Le PSC doit-il fournir cet exemplaire avant d'inscrire le certificat dans l'annuaire électronique ? Le cas échéant, doit-il obtenir l'acceptation préalable du candidat titulaire ? L'exposé des motifs pourrait le laisser penser. Ce dernier précise en effet que cette obligation permet au « candidat titulaire de vérifier le contenu du certificat et de le valider. Dès l'acceptation acquise, le PSC peut inscrire le certificat dans l'annuaire électronique. A partir de ce moment, il est opposable aux tiers »[79]. Nous attirons néanmoins l'attention du lecteur sur le fait que ce commentaire porte sur une disposition – existant dans le premier projet de loi – qui obligeait le PSC à obtenir une acceptation préalable mais qui n'a pas, on ne sait pour quelle raison, été reprise dans la loi. Il est donc probable que l'obligation prescrite par l'article 9 laisse plus de latitude au PSC que ne le suggère l'exposé des motifs.

Conservation d'un annuaire électronique – Selon l'article 10, le PSC est très logiquement tenu de « conserver un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration ». Cette obligation basique est complétée par d'autres obligations dissimulées dans l'annexe II. En effet, le point b) de cette annexe précise que le fonctionnement du service d'annuaire doit être rapide et sûr, ce qui suppose que les utilisateurs puissent y accéder en permanence par voie électronique et obtenir rapidement le certificat souhaité. Le point c) stipule que le PSC doit veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision. On en déduit que ces informations doivent être accessibles de la même manière que le certificat lui-même[80]. Par ailleurs, on présume que la responsabilité du PSC ne peut pas être engagée pour les conséquences dommageables résultant de l'utilisation du certificat en dehors de sa période de validité. Le point l) est, quant à lui, encore plus contraignant et complexe.

En effet, le point l) impose au PSC d'utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable – ce qui suppose l'accès et la consultation aisée du certificat recherché – de sorte que quatre conditions soient remplies. Premièrement, seules les personnes autorisées doivent pouvoir introduire et modifier des données. L'octroi de pouvoirs

[79] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 30.
[80] On relève à cet égard le point f) de l'annexe I qui prévoit que le certificat doit comporter l'indication du début et de la fin de la période de validité du certificat.

exclusifs à certaines personnes (administrateur(s) de la base de données de certificats) et l'utilisation par le PSC de procédures d'accès sécurisées devraient permettre de répondre aisément à cette condition. Deuxièmement, il doit être possible de contrôler « l'authenticité » de l'information. Sur ce point, la signature électronique avancée du certificat par le PSC devrait permettre à l'utilisateur de vérifier tant le contenu que l'origine du certificat (annexe I, point h). Le cas échéant, encore faut-il que le certificat du PSC soit lui même certifié ! La loi ne souffle mot sur ce point. On peut imaginer une certification par l'Administration voire une certification croisée entre PSC. Troisièmement, les certificats ne peuvent être disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement. Cette obligation doit être bien comprise. On a probablement voulu éviter que toute personne puisse utiliser l'annuaire afin d'effectuer des recherches générales sur l'ensemble des personnes ayant obtenu un certificat et accéder ainsi à certaines données à caractère personnel (identité, attributs spécifiques divers). Par ailleurs, on peut comprendre que les PSC ne soient pas favorables à ce qu'un concurrent puisse à tout moment consulter la liste complète des certificats émis par lui, obtenir ainsi l'identité de leur titulaire et, en quelque sorte, accéder de cette manière à sa « base de données clients » ! Toutefois, cette obligation ne fait évidemment pas obstacle à ce qu'un destinataire de message signé électroniquement puisse accéder à tout moment à l'annuaire pour rechercher un certificat précis et vérifier que celui-ci n'est pas révoqué ou expiré. En pratique, cela peut se faire en indiquant le code d'identité du certificat (numéro de série), éventuellement communiqué par le signataire du message, dans la requête de vérification du certificat. La réponse à cette requête par le PSC indique alors si le certificat appartient effectivement au signataire et s'il est toujours valide. Cette technique évite à quiconque de pouvoir accéder aux autres certificats n'ayant aucun lien avec le message envoyé. Quatrièmement, il est nécessaire que toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur. Il s'agit là d'une obligation abstraite qui devra être concrétisée par l'utilisation d'outils informatiques adéquats. On relève l'utilisation du mot « opérateur » dont on ne sait pas, à vrai dire, s'il vise le PSC ou l'utilisateur du certificat. On présume qu'il s'agit du PSC.

On souligne que, de manière surprenante, la loi ne dit rien quant à l'exigence et aux conditions d'interopérabilité des annuaires électroniques de certificats conservés par les PSC concurrents ! Or la concurrence ne sera véritable et l'utilisation généralisée de la signature électronique ne sera possible que lorsqu'il existera une véritable interopérabilité entre les différents annuaires. En attendant, les clients d'un PSC pourront difficilement, en raison d'obstacles techniques, envoyer et vérifier des messages signés électroniquement à des clients d'un autre PSC, et inversement.

b) Le respect des exigences des annexes I et II (art. 11)

L'article 11 détermine les conditions relatives aux certificats qualifiés. « Les certificats qualifiés doivent satisfaire aux exigences visées à l'annexe I » (art. 11, § 1er). De plus, « Les PSC qui délivrent des certificats qualifiés doivent satisfaire aux exigences visées à l'annexe II » (art. 11, § 2). Nous ne voyons pas ce qu'ajoute cet article par rapport à la définition donnée du certificat qualifié, qui consacrait déjà ces deux obligations (art. 2, 4°, cf. *supra*). Nous profitons néanmoins de cette redondance pour commenter les points des annexes n'ayant pas encore fait l'objet de développements.

L'annexe I énumère les informations devant impérativement figurer sur le certificat qualifié. Le premier élément consiste à garantir la transparence en indiquant la mention selon laquelle le certificat est délivré au titre de certificat qualifié. Cette information est primordiale pour le

PSC, dont le régime juridique dépend essentiellement du caractère qualifié ou non des certificats qu'il émet. Elle est également importante non seulement pour le titulaire du certificat mais également pour le destinataire d'un message signé électroniquement car elle permet de garantir à ceux-ci que le certificat sur lequel se fonde la signature électronique remplit une des conditions pour pouvoir bénéficier de la clause d'assimilation.

Le certificat qualifié doit également comporter l'identification du PSC ainsi que le pays dans lequel il est établi. L'indication de la nationalité permet notamment de déterminer l'Administration qui est compétente pour exercer son pouvoir d'injonction dans le cadre du contrôle des PSC – l'Administration belge ne peut par exemple mettre en demeure que les PSC établis en Belgique (art. 20, § 3) – et joue également un rôle dans le cadre de la reconnaissance transfrontière des certificats (voy. notamment l'article 16, § 2, point a).

Si la mention « certificat qualifié » n'est pas indiquée dans le certificat, il va de soi que ce dernier ne permet pas à son titulaire de bénéficier de la clause d'assimilation. Si l'une des autres mentions telle l'identité de son titulaire venait à manquer, le certificat pourrait ne pas accéder au statut de certificat qualifié et son titulaire risquerait de ne pas pouvoir jouir des effets juridiques reconnus à ce type de certificat (cf *supra*), encore même celui-ci indiquerait-il la mention selon laquelle il est émis au titre de certificat qualifié. Dans cette hypothèse, il se peut qu'un titulaire s'aperçoive après coup que les moyens de preuve électroniques qu'il s'était préconstitué ne bénéficient pas, après analyse, de la clause d'assimilation ! S'il est vrai que les risques de la survenance d'une telle situation sont limités en raison, d'une part, du pouvoir de contrôle de l'Administration qui peut vérifier que les PSC émettant des certificats qualifiés respectent toutes les exigences de la loi, d'autre part, du fait que l'article 14 consacre une présomption de responsabilité à charge du PSC dans ce cas (art. 14, § 1er, point a), il n'empêche qu'on se trouve en présence d'un maillon faible en terme de sécurité juridique. Par contre, si une mention moins importante, tels le code d'identité du certificat ou la mention pseudonyme, venait à manquer, il nous semble que le certificat devrait conserver le statut de certificat qualifié et permettre à son titulaire et/ou à la personne qui se fie à ce certificat de bénéficier des effets juridiques qui en découlent. Le PSC, quant à lui, pourrait voir sa responsabilité engagée pour avoir délivré des certificats sans avoir vérifié leur complétude (cf. *infra*).

L'annexe I stipule aussi que le certificat qualifié doit comporter la signature électronique avancée du PSC qui délivre le certificat. Cela signifie que le prestataire va signer le certificat avec ses propres données afférentes à la création de signature afin que l'utilisateur du certificat puisse s'assurer que les informations ont été certifiées par tel ou tel prestataire et que l'intégrité de ces informations est sauvegardée. Cette condition permet en pratique d'assurer le respect de deux exigences contenues dans l'annexe II selon lesquelles le PSC doit prendre des mesures *contre la contrefaçon* des certificats (point g) mais aussi utiliser des systèmes fiables pour stocker les certificats de sorte que *l'information puisse être contrôlée quant à son authenticité* (point l, sous-point b).

Le texte ne dit pas si la liste des exigences concernant les certificats qualifiés de l'annexe I est limitative. *A priori*, nous ne voyons aucun obstacle à ce qu'un PSC intègre d'autres informations supplémentaires que celles prévues dans l'annexe I. Sans doute peut-on considérer cette liste comme minimale. Toutefois, il nous semble que l'ajout de mentions ne devrait pas avoir pour effet de « noyer » les mentions obligatoires dans une masse d'informations présentant moins d'intérêt.

Tout PSC qui désire émettre des *certificats qualifiés* doit, au-delà de l'annexe I, également se conformer aux prescriptions de l'annexe II. Ces dernières tendent à garantir la sécurité du mécanisme de certification et des activités du prestataire. Nous nous limitons à présenter certaines garanties de l'annexe II qui n'ont pas encore fait l'objet d'un commentaire préalable. Nous pouvons résumer ces garanties comme suit.

Garanties de sécurité et de fiabilité – Le PSC doit « faire la preuve qu'il est suffisamment fiable pour fournir des services de certification » (annexe II, point a). Dans un domaine à ce point technique et en perpétuelle évolution, on imagine le malaise que peuvent ressentir les PSC face à une obligation aussi vague. A partir de quand peut-on dire que le niveau de fiabilité suffisant est atteint ? Sur la base de quels critères ? Qui apprécie la suffisance du niveau de fiabilité ? Dans le cadre d'une demande d'accréditation, on comprend que l'Administration joue un rôle déterminant (et discrétionnaire ?) à cet égard. Par contre, on sait qu'un PSC peut d'initiative émettre des certificats qualifiés indépendamment de toute accréditation, et donc sans devoir obtenir une autorisation préalable d'une autorité. Dans ce cas, il aurait été plus judicieux d'indiquer que le PSC doit « *être en mesure de* faire la preuve …», par exemple dans le cadre d'un contrôle de l'Administration, car le fait d'apporter activement la preuve de sa fiabilité n'est pas en soi une condition préalable à l'émission de certificats qualifiés.

Le PSC doit « utiliser des systèmes et produits fiables » (annexe II, point f). Rappelons que lorsqu'un PSC utilise un produit conforme aux normes publiées au *J.O.C.E.*, le critère de fiabilité est présumé respecté (cf. *supra*).

Enfin, le PSC doit posséder l'expertise nécessaire pour assurer ses activités de certification. A cette fin, il emploie du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences et connaissances en gestion et en technologie des signatures électroniques ainsi qu'une bonne pratique des procédures de sécurité appropriées. Il doit en outre appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues (annexe II, point e).

Garanties d'information – Rappelons que l'objectif de la loi est de renforcer la confiance et de promouvoir l'utilisation de la signature électronique dans un cadre sécurisé. L'information correcte de l'utilisateur des services contribue à la réalisation de cet objectif. Ainsi, le PSC a l'obligation de procurer toute information nécessaire à l'utilisation correcte et sûre de ses services, et cela « avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique » (annexe II, point k). Plus précisément, le PSC est tenu d'informer le candidat titulaire « des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges ». Ce dernier point est intéressant car il semble imposer indirectement aux PSC qui délivrent des certificats qualifiés de mettre en place des procédures de réclamation et de règlement des litiges, ou, à tout le moins de faire appel à un tiers qui offre ce type de services.

Ces informations doivent être fournies dans une « langue aisément compréhensible ». L'exposé des motifs précise que le PSC doit fournir ces informations au moins dans la ou les langues officielles du pays dans lequel il est établi ainsi que dans une ou plusieurs langues

internationales[81]. La loi autorise la transmission de ces informations par voie électronique mais, le cas échéant, elles doivent être fournies par un moyen de communication durable. On vise probablement par ces termes de nouvelles formes de communication, susceptibles de remplacer l'écrit traditionnel, qui rentrent, selon l'exposé des motifs[82], dans la notion de support durable telle qu'utilisée dans certains textes européens ou nationaux (ce concept englobe par exemple les disquettes informatiques, les CD-ROM, ainsi que le disque dur de l'ordinateur du consommateur stockant des courriers électroniques)[83].

Garanties financières – Le PSC doit posséder des ressources financières suffisantes pour exercer ses activités et, le cas échéant, indemniser les utilisateurs ayant subi un dommage suite à l'inexécution des obligations qui lui sont imposées par ou en vertu de la loi (annexe II, point h). Cette obligation impose-t-elle au PSC de souscrire une police d'assurance appropriée ? Rien n'est moins sûr. Le point h) de l'annexe II semble suggérer que la souscription d'un contrat d'assurance est un moyen, parmi d'autres, de satisfaire à cette obligation[84]. Par contre, l'article 4, § 2, semble plus catégorique dans sa formulation en ce sens que les PSC qui délivrent des certificats qualifiés sont tenus de communiquer à l'Administration « la preuve qu'une assurance a été souscrite en vue de couvrir leurs obligations visées à l'article 14 » ! Cela nous semble excessif dans la mesure où le contrat d'assurance n'est pas le seul outil disponible qui permette d'offrir la garantie de ressources financières suffisantes[85].

Garanties probatoires – Afin principalement de pouvoir fournir une preuve de la certification en justice, le PSC est tenu « d'enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile de 30 ans » (annexe II, point i). Le texte ne précise pas ce qu'il faut entendre par « informations pertinentes ». On présume qu'il s'agit notamment des informations contenues dans le certificat (identité du titulaire, attributs spécifiques éventuels, limites d'utilisation éventuelles…) ainsi que des différents documents probants ayant permis de vérifier l'exactitude de ces informations, la date d'émission et d'expiration du certificat, la date de révocation éventuelle, les coordonnées exactes du titulaire dans l'hypothèse où il utilise un pseudonyme, le registre des personnes physiques visé à l'article 8, § 3, en cas de délivrance de certificats à une personne morale… Vu la masse d'informations à conserver et la durée importante de conservation, la loi indique que « ces enregistrements peuvent être effectués par des moyens électroniques »[86]. Cette possibilité offre une grande

---

[81] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 29.

[82] *Ibidem.*

[83] Pour une analyse fouillée et critique de cette notion, nous renvoyons à l'article de M. DEMOULIN, « La notion de *support durable* dans les contrats à distance : une contrefaçon de l'écrit », *Rev. eur. dr. cons.*, 4/2000, pp. 361-377. Voy. également, M. DEMOULIN, « Information et transparence sur les réseaux » in *Le commerce électronique sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, sous la direction du Professeur E. MONTERO, Cahiers du CRID, n° 19, Bruxelles, Bruylant, 2001, pp. 125 et s.

[84] Le point h), de l'annexe II indique en effet « …en contractant, *par exemple*, une assurance appropriée ».

[85] P. LECOCQ et B. VANBRABANT estiment, quant à eux, qu'il est malheureux que le législateur n'ait « que suggéré et non imposé la souscription d'une assurance de responsabilité » (« La preuve du contrat conclu par voie électronique » *in Le commerce électronique : un nouveau mode de contracter ?*, Editions du jeune barreau de Liège, 2001, p. 101).

[86] Les documents papiers pourraient par exemple être numérisés et conservés sur un support durable. Nous attirons toutefois l'attention sur les difficultés techniques de conserver un document électronique pendant une durée de 30 ans. Sur ce point, nous renvoyons le lecteur au rapport de la commission 4 sur le droit de la preuve rédigé dans le cadre du projet e-Justice (M. DEMOULIN, D. GOBERT, C. LAZARO et O. LEROUX, sous la direction du professeur Y. POULLET, rapport final sur le droit de la preuve, projet e-Justice, disponible à l'adresse suivante : http://www.droit.fundp.ac.be/e-justice/default.htm).

souplesse au PSC dans les méthodes de gestion de ses archives. Par ailleurs, elle garantit sans équivoque au PSC la valeur probatoire des documents présentés au juge sous forme électronique. Le texte ne précise pas le point de départ du délai de conservation. A l'instar de Pascale Lecocq et Bernard Vanbrabant[87], nous pensons qu'il démarre au moment de la génération de la dernière information pertinente relative au certificat, à savoir la date d'expiration du certificat, ou éventuellement sa date de révocation, et non sa date d'émission. Enfin, notons que le PSC reste tenu de cette obligation de conservation même s'il cesse ses activités (art. 15).

Garanties d'interopérabilité - Enfin, la Commission européenne indique, dans sa communication du 8 octobre 1997[88] et dans le considérant numéro 5 de la directive sur les signatures électroniques, que l'interopérabilité des différents systèmes et applications de signatures électroniques est absolument nécessaire afin d'assurer que celles-ci puissent être mises en œuvre en Europe et en dehors de l'Europe. Nous constatons néanmoins qu'il s'agit essentiellement d'une déclaration d'intention car cette exigence d'interopérabilité ne se retrouve ni dans le texte des articles de la directive ni dans la loi belge. Espérons que le comité d'experts chargé, en vertu de l'article 3, § 5, et de l'article 9 de la directive, de déterminer les normes généralement admises, veillera à prendre en compte l'exigence d'interopérabilité des produits de signature électronique.

c) **La révocation des certificats qualifiés (art. 12 et 13)**

Un certificat a généralement une durée de vie limitée. Il contient une date d'expiration, indiquée dans le certificat lui-même. A cet égard, la loi impose au PSC d'en informer, un mois avant l'expiration d'un certificat, son titulaire (art. 12, § 2, al. 2). Pour diverses raisons, il est possible que l'on doive parfois mettre anticipativement un terme à un certificat. Le cas échéant, on procède à sa révocation aux conditions et selon les modalités des articles 12 et 13. La révocation est, d'un point de vue technique, assurée par le PSC qui a délivré le certificat soit à la demande du titulaire (art. 12, § 1er) soit d'office si certaines conditions le justifient (art. 12, § 2).

La demande de révocation peut être effectuée par le titulaire lui-même. Il ne semble pas que cette demande doive être motivée. Il peut donc la faire de manière discrétionnaire – sans raisons objectives – ou en application de son obligation de révocation « en cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat » (art. 19, § 2). Le cas échéant, le PSC est tenu à une double obligation. Il ne peut tout d'abord procéder à la révocation qu'après avoir préalablement vérifié que la personne qui fait la demande est effectivement le titulaire du certificat[89]. Il nous semble que cette vérification d'identité ne doit pas être accomplie de manière aussi contraignante que cela ne l'était pour la délivrance du certificat. En raison généralement de l'urgence de devoir procéder à la révocation, une identification sommaire mais raisonnable devrait suffire[90]. Ensuite, il est tenu de révoquer

[87] P. LECOCQ et B. VANBRABANT, *op.cit.*, p. 97, note 145.

[88] COM(97)503 : Vers un Cadre Européen pour les Signatures Numériques et le Chiffrement : Assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997, p. 21.

[89] L'article 12, § 1er, indique en effet « A la demande du titulaire du certificat, préalablement identifié, … ».

[90] Si elle se fait en ligne, on peut inviter le demandeur à signer sa demande de révocation à l'aide de sa signature électronique ou utiliser un autre moyen d'identification. Par contre, si elle se fait autrement, par exemple par téléphone ou par fax, on pourrait demander au titulaire de communiquer une information que les tiers ne sont

immédiatement le certificat. Par les mots « révoquer immédiatement », on présume que la loi a voulu dire « inscrire immédiatement la mention de la révocation du certificat dans l'annuaire électronique » au sens de l'article 13, § 2. S'il ne le fait pas, sa responsabilité est engagée dans les conditions de l'article 14, § 2. Dans ce cadre, nous ne pouvons que conseiller aux PSC de conserver la preuve de la réalité et de la date d'une demande de révocation afin qu'il puisse aisément démontrer, si nécessaire, que la révocation a été opérée immédiatement après la demande.

Il peut aussi arriver qu'un certificat soit révoqué à l'initiative du PSC ayant délivré ce dernier. En effet, le PSC a l'obligation de procéder à la révocation dans quatre hypothèses[91] (art. 12, § 2).

Premièrement, il doit le faire s'il « existe des raisons sérieuses pour admettre que le certificat a été délivré sur base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée » (art. 12, § 2, 1°). Vu le libellé du texte, et à l'instar de la philosophie des règles de responsabilité consacrées par la directive sur le commerce électronique[92], il ne semble pas exister d'obligation générale de surveillance à charge du PSC, à tout le moins après la délivrance du certificat. Le PSC n'est donc pas tenu, une fois le certificat délivré, de vérifier de manière active et périodique que les informations contenues dans le certificat sont toujours exactes ou que le titulaire veille correctement à la confidentialité des données utilisées pour signer ! Par contre, il doit révoquer le certificat s'il constate fortuitement ou s'il est averti par un tiers que les conditions de révocation sont remplies (par exemple, un ordre professionnel, jouant le rôle d'autorité d'enregistrement ou non, informe le PSC que le titulaire s'est retiré ou a été radié de l'ordre et que par conséquent l'attribut spécifique indiqué dans le certificat n'est plus conforme à la réalité[93]).

Deuxièmement, le PSC doit également révoquer les certificats lorsque les tribunaux ont ordonné à son égard les mesures prévues à l'article 20, § 4, b)[94] (art. 12, § 2, 2°). En effet, si un PSC délivre des certificats qualifiés dans le non respect de la loi, l'Administration peut le mettre en demeure de régulariser la situation endéans un délai raisonnable. Si le PSC ne prend pas les mesures nécessaires dans ce délai, l'Administration peut alors saisir les tribunaux pour qu'ils prennent des mesures telles que notamment l'injonction au PSC d'informer immédiatement les titulaires des certificats qualifiés de leur non-conformité avec la loi. En raison de cette non-conformité, il était logique d'imposer au PSC la révocation de certificats qui ne remplissent pas toutes les conditions pour pouvoir revendiquer le statut de certificats *qualifiés*.

---

pas censés connaître (telle qu'un mot de passe communiqué pour cette hypothèse lors de la demande de certificat ou une information personnelle comme une date de naissance).

[91] Dès lors que les conditions sont remplies, il s'agit selon nous d'une obligation de révocation à charge du PSC et non d'un simple droit. En sens contraire, J.F. LEROUGE et Y. POULLET, « La responsabilité des acteurs de l'Internet », *à paraître* in Rapports belges au Congrès de droit comparé de Brisbane (juillet 2002), Bruylant, Bruxelles, 2002, note 86.

[92] Sur ce point voy. E. MONTERO, « La responsabilité des prestataires intermédiaires sur les réseaux », in *Le commerce électronique sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, sous la direction du Professeur E. MONTERO, Cahiers du CRID, n° 19, Bruxelles, Bruylant, 2001, pp. 279 et s.

[93] Sur ce point, nous ne pouvons que conseiller au PSC de créer contractuellement une obligation à charge de l'autorité d'enregistrement de l'informer de la perte d'un attribut, spécialement lorsque cette perte peut résulter d'une décision de cette dernière et non du titulaire, comme c'est le cas pour les ordres professionnels.

[94] On s'interroge sur l'intérêt de prévoir ce point b). Faire référence à l'article 20, § 4, aurait, selon nous, été suffisant.

Troisièmement, le PSC procède nécessairement à la révocation des certificats lorsqu'il « arrête ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de service de certification garantissant un niveau de qualité et de sécurité équivalent » (art. 12, § 2, 3°). Cette obligation est redondante avec la même obligation stipulée à l'article 15, § 1er, qui ajoute néanmoins que la révocation doit avoir lieu « deux mois après en avoir averti les titulaires ».

Quatrièmement, le PSC révoque le certificat lorsqu'il « est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire » (art. 12, § 2, 4°). Cette hypothèse est logique : on ne peut maintenir un certificat qui identifiait une personne morale qui n'existe plus juridiquement de la même manière que n'est pas transmissible pour cause de mort un certificat qui appartenait à une personne physique. Soulignons que la loi ne vise pas l'hypothèse de la fusion de société. Une société absorbée par une autre société peut-elle conserver ses certificats, en demandant éventuellement au PSC de modifier son identité sociale ? Cette possibilité est peu recommandable, notamment en raison de la possible confusion que cela pourrait engendrer. Même si les activités et le personnel de la société absorbée restent identiques, on se trouve néanmoins en présence d'une nouvelle société – ayant une identité distincte, un patrimoine juridique propre, des organes de gestion différents – qui mérite la délivrance de nouveaux certificats individualisés. De toute manière, l'article 12, § 2, 1°, qui impose au PSC de révoquer le certificat lorsque les informations ne sont plus conformes à la réalité, trouverait probablement à s'appliquer dans l'hypothèse d'une fusion.

Dans le cas où le PSC révoque un certificat dans le cadre d'une de ces quatre hypothèses, il est tenu d'en informer le titulaire[95] mais surtout de motiver sa décision (art. 12, § 2, al. 2). Cette motivation s'avère particulièrement importante lorsque le PSC révoque un certificat sur la base de l'article 12, § 2, 1°. En effet, le PSC a tout intérêt à préciser l'ensemble des raisons sérieuses qui l'ont amené à croire que le certificat a été délivré sur base d'informations erronées ou falsifiées, ou que les informations contenues dans le certificat ne sont plus conformes à la réalité voire même que la confidentialité des données afférentes à la création de signature a été violée. Dans l'hypothèse où un titulaire contesterait la légitimité d'une telle révocation, il nous semble que ce n'est que dans des cas extrêmes que ce dernier devrait pouvoir prouver le caractère abusif de la révocation, et obtenir le cas échéant réparation du préjudice. Ce serait le cas si le titulaire apportait le preuve que le PSC a révoqué le certificat « à la légère » – en l'absence de *raisons sérieuses* – ou sur la base d'autres motivations – moins avouables – que celles consacrées par le point 1 du paragraphe 2 de l'article 12[96]. Selon nous, il convient donc de ne pas sanctionner trop rapidement un PSC qui aurait – par application du principe de précaution ou par crainte que l'on lui reproche de ne pas avoir respecté ses obligations de l'article 12 – révoqué le certificat hâtivement et sans analyse approfondie des causes qui justifient cette révocation, même s'il doit malgré tout pouvoir justifier de « raisons sérieuses ».

[95] On notera que la loi n'exige pas dans ce cas que l'information soit préalable à la révocation (sauf lorsque la révocation résulte de la cessation volontaire par le PSC de ses activités). Elle peut se faire de manière concomitante à la révocation voire même après celle-ci, mais alors dans un très bref délai selon nous.

[96] Un PSC qui invoquerait qu'il a des raisons de croire que la confidentialité des données afférentes à la création de signature a été violée pour révoquer le certificat alors qu'en réalité, il s'agit d'un subterfuge pour écarter un client insuffisamment rentable.

L'article 12, § 3, précise que « la révocation d'un certificat est définitive »[97]. La décision de révocation est irréversible. Il n'est donc pas possible de « ressusciter » un certificat, spécialement après l'indication de la mention de la révocation de ce dernier dans l'annuaire électronique. Le cas échéant, le titulaire d'un certificat révoqué, à son initiative ou d'office par le PSC, doit faire une nouvelle demande de certificat. Dans ce cas, il ne peut évidemment pas faire certifier les mêmes données afférentes à la vérification de signature (art. 19, § 3).

Notons que par souci de sécurité juridique, et malgré une tentative avortée d'amendement du texte au Sénat[98], la loi n'a pas mis en place une procédure de suspension des certificats. Par ailleurs, les travaux préparatoires semblent même exclure que le PSC puisse mettre en place une telle procédure, à tout le moins pour les certificats qualifiés[99].

L'obligation à charge du PSC de procéder techniquement à la révocation des certificats n'est pas minime. Elle suppose que le PSC prenne « les mesures nécessaires afin de répondre à tout moment et sans délai » à une telle demande (art. 13, § 1er). Les travaux parlementaires précisent quelque peu cette obligation comme suit : « Le PSC doit être en mesure de traiter en permanence (vingt-quatre heures sur vingt-quatre) les demandes de révocation et d'y donner suite immédiatement. A cette effet, le PSC assure que des moyens appropriés sont à la disposition du titulaire pour effectuer une demande de révocation »[100]. Qu'entend-on par « moyens appropriés » ? Les travaux parlementaires ne s'étendent malheureusement pas sur ce point. Il ne nous semble pas qu'un système en ligne de révocation constitue, à lui seul, les moyens appropriés exigés par la loi. En effet, on sait que les données afférentes à la création de signature sont généralement stockées sur une carte à puce. Par exemple, en cas de vol de celle-ci, il ne nous semble pas déraisonnable de permettre au titulaire de pouvoir demander la révocation par téléphone ou par téléfax, à l'instar de ce qui se fait actuellement dans le monde bancaire. Ce sont effectivement des moyens beaucoup plus facilement et rapidement accessibles qu'un ordinateur équipé d'internet, à tout le moins tant que nos coins de rues ne seront pas équipés d'une « cyber-borne ».

Par ailleurs, le PSC est tenu d'inscrire dans l'annuaire électronique la mention de la révocation du certificat, immédiatement après la décision de révocation (art. 13, § 2, al. 1). La révocation est opposable aux tiers à partir de cette inscription[101] (art. 13, § 2, al. 2). Il en résulte que le destinataire d'un message qui se fie à un message signé électroniquement après cette inscription pourra difficilement engager la responsabilité du titulaire ou du PSC, sauf à prouver que le titulaire a continué à utiliser les données afférentes à la création de signature et le certificat en violation de l'article 19, § 3, ou que la mention, selon laquelle le certificat est révoqué, n'est pas visible.

d) **La responsabilité des prestataires (art. 14)**

Les dispositions relatives à la responsabilité des PSC sont particulièrement importantes car elles conditionnent en partie la confiance que les utilisateurs pourront placer dans un régime de certification.

---

[97] Comme le confirme l'exposé des motifs, le caractère définitif de la révocation est relatif au certificat qui est révoqué. Cela ne fait évidemment pas obstacle à la possibilité pour l'ex-titulaire d'introduire une nouvelle demande de certificat, voy. *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, p. 14.

[98] Amendements n° 7 et 8 de M. Steverlynck, *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/2, pp. 3 et 4.

[99] *Doc. parl.*, Sén., sess. ord. 2000-2001, n° 2-662/4, pp. 13 et 14.

[100] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 35.

[101] Ce moment sera en principe connu aisément par les tiers puisque l'annexe II, point c), impose au PSC de veiller à ce que la date et l'heure de la révocation d'un certificat puissent être déterminées avec précision.

Le régime juridique mis en place par la directive, repris servilement par l'article 14 de la loi, tente d'établir un équilibre entre les intérêts des prestataires de service de certification et ceux des utilisateurs de certificats afin que le régime de certification établi présente un haut degré de fiabilité et, par là même, de crédibilité, sans qu'il entrave pour autant le développement de la certification et, par conséquent, du commerce électronique[102]. Avant de présenter ce régime, il convient de délimiter le champ d'application des dispositions relatives à la responsabilité.

1) Champ d'application

La loi, conformément à la directive, ne traite des questions relatives à la responsabilité qu'à propos des certificats émis par les PSC qui délivrent à l'intention du public des certificats présentés comme *qualifiés* ou qui garantissent publiquement de tels certificats[103]. Dès lors, pour les PSC qui délivrent des certificats ordinaires – qui ne sont pas présentés comme qualifiés –, le droit commun de la responsabilité trouve à s'appliquer[104]. La différence de régime de responsabilité – dont nous verrons qu'elle n'est pas fondamentale par rapport aux règles de droit commun de la responsabilité – s'explique probablement par le fait que des conséquences juridiques propres sont attachées aux certificats qualifiés.

Par ailleurs, le régime de responsabilité spécifique établi par la loi ne vise que les relations entre les PSC et les destinataires de certificats qualifiés, c'est-à-dire « toute personne qui se fie raisonnablement au certificat »[105]. La loi ne semble donc pas traiter des questions relatives à la responsabilité qui pourraient se poser dans le cadre des relations entre les PSC et les titulaires de certificats[106], ni aux relations éventuelles entre PSC et autorités d'enregistrement ou autres sous-traitants. Ici aussi, à défaut de règles spécifiques, le droit commun de la responsabilité trouve à s'appliquer, avec la possibilité pour le PSC de prévoir des clauses exonératoires ou limitatives de responsabilité sous réserve bien entendu des limites jurisprudentielles classiques[107].

---

[102] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 36 et considérant n° 14 de la directive européenne en la matière.

[103] Sur ce dernier point, nous renvoyons le lecteur au commentaire de l'article 16 de la loi relatif aux certificats délivrés au titre de certificats qualifiés par des PSC étrangers (cf. *infra*).

[104] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 36 et considérant n° 22 de la directive européenne. De manière générale, il nous semble que la responsabilité d'un PSC doit s'apprécier en fonction du degré de confiance que l'on peut accorder à celui-ci. Si le certificat n'accède pas au statut de certificat qualifié, et que par la force des choses le PSC ne remplit pas les exigences pour ce faire, il est logique que les parties qui utilisent ledit certificat – son titulaire et la personne qui se fie au certificat – ne peuvent s'attendre au même niveau de fiabilité du certificat et, par conséquent, au même niveau de responsabilité du PSC.

[105] M. ANTOINE et D. GOBERT, « La directive européenne sur la signature électronique : vers la sécurisation des transactions sur l'Internet ? », *J.T.D.E.*, 2000, n° 68, p. 76.

[106] Par contre, il est vrai que ces règles sont de nature à alléger la responsabilité contractuelle (apparente) du titulaire envers le destinataire dans la mesure où il pourrait être délié d'un engagement pris à son nom suite à une faute du PSC.

[107] Pour une synthèse récente des limites assignées par la jurisprudence à la validité des clauses exonératoires ou limitatives de responsabilité, E. MONTERO, « Les clauses limitatives ou exonératoires de responsabilité. Rapport belge », in M. FONTAINE et G. VINEY (dir.), *Les sanctions de l'inexécution des obligations contractuelles. Etudes de droit comparé*, Bruxelles-Bruylant, Paris-L.G.D.J., 2001, pp. 393-434.

2) Responsabilité des PSC délivrant des certificats qualifiés

L'article 14 règle la responsabilité des PSC à l'égard des destinataires de messages signés électroniquement ou, pour reprendre les termes de la loi, à l'égard de « tout organisme ou personne physique ou morale qui, en bon père de famille, se fie raisonnablement au certificat ». Comme le soulignent Pascal Lecocq et Bernard Vanbrabant, c'est la « responsabilité extracontractuelle des certificateurs » qui est envisagée ici[108]. Plus précisément, la loi établit une présomption de responsabilité dans le chef du PSC dans les trois domaines suivants : l'exactitude et la complétude des informations contenues dans le certificat, la vérification de la détention et de la complémentarité des données afférentes à la création de signature et, enfin, l'enregistrement de la révocation des certificats[109]. Comme dit précédemment, la présomption de responsabilité joue pour tout préjudice causé à toute personne qui, en bon père de famille, se fie raisonnablement au certificat.

Exactitude et complétude des informations contenues dans le certificat – Les PSC qui délivrent à l'intention du public des certificats présentés comme qualifiés, ou qui garantissent publiquement de tels certificats, doivent garantir « l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré » (art. 14, § 1er, a). Puisqu'une obligation d'exactitude pèse sur le prestataire à ce moment précis, il doit veiller à ce que la date et l'heure d'émission du certificat puissent être déterminées avec précision (annexe I, point f et annexe II, point c). Par ailleurs, on notera que l'obligation d'exactitude pèse sur l'ensemble des informations contenues dans le certificat, et pas uniquement sur celles qui doivent obligatoirement y figurer en vertu de l'annexe I[110]. Le fait que les informations mentionnées sur le certificat soient bien souvent vérifiées par un tiers, l'autorité d'enregistrement, et non par le prestataire ne change rien à la responsabilité de ce dernier[111] (cf. *supra*). Les PSC doivent également veiller à garantir « la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié », c'est-à-dire de toutes les mentions prescrites par l'annexe I[112].

Si la loi prévoit une obligation d'exactitude des informations contenues dans le certificat au moment précis de son émission, et non à dater de ce moment, c'est parce qu'il ne peut raisonnablement être demandé au PSC d'assurer, une fois le certificat délivré, un contrôle permanent des informations contenues dans le certificat[113]. Après la délivrance, un devoir de

---

[108] P. LECOCQ et B. VANBRABANT, *op.cit.*, p. 99.

[109] Sur ces points, voy. M. ANTOINE et D. GOBERT, *op.cit.*, *J.T.D.E.*, 2000, p. 76 ; M. E. STORME, « De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen », *R.W.*, 9 juin 2001, n° 41, pp. 1505-1525 ; J.F. LEROUGE et Y. POULLET, « La responsabilité des acteurs de l'Internet », *à paraître* in Rapports belges au Congrès de droit comparé de Brisbane (juillet 2002), Bruylant, Bruxelles, 2002 ; J. DUMORTIER et S. VAN DEN EYNDE, « De juridische erkenning van de elektronische handtekening in België », *Computerrecht*, 2001/4, p. 193.

[110] En ce sens, J.F. LEROUGE et Y. POULLET, *op.cit.*.

[111] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 37. Nous ne pouvons que conseiller au PSC de régler par convention avec l'autorité d'enregistrement toutes les hypothèses donnant le droit au PSC de se retourner contre elle au cas où sa responsabilité serait engagée suite à une erreur de l'autorité d'enregistrement.

[112] Si la mention selon laquelle le certificat est délivré au titre de certificat qualifié ne se trouve pas dans celui-ci, le régime de responsabilité visé à l'article 14 ne trouve en principe pas à s'appliquer. Toutefois, un bémol doit être apporté à cette affirmation. En effet, on devrait pouvoir faire application de la présomption de responsabilité consacrée à l'article 14 à l'égard d'un PSC qui prétend sur son site web et sur ses prospectus publicitaires par exemple émettre des certificats qualifiés alors qu'il omet systématiquement d'indiquer ladite mention dans les certificats qu'il délivre !

[113] En ce sens, M. ANTOINE et D. GOBERT, *J.T.D.E.*, *op.cit.*, p. 76 ; J.F. LEROUGE et Y. POULLET, *op.cit.*

vigilance pèse donc sur le titulaire du certificat. Il doit notamment informer le PSC ayant émis le certificat de toute modification relative aux données du certificat et, conformément à l'article 19, § 2, demander la révocation de ce dernier.

Détention et complémentarité des données afférentes à la création et à la vérification de signature – Le PSC doit « s'assurer, au moment de la délivrance du certificat, que le signataire[114] identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat » (art. 14, § 1er, b).

L'obligation de vérification dont il est question ci-dessus pèse sur tout PSC, qu'il soit ou non chargé de générer les données afférentes à la création et à la vérification de signature. L'obligation de vérification de la détention des données précitées sous-tend-elle l'obligation de vérification de leur complémentarité ? L'article 8, § 1er, apporte une réponse affirmative à cette question. Le PSC est tenu de vérifier la complémentarité des données, sans faire de distinction selon que le PSC a généré lui même les données ou que celles-ci ont été communiquées par le demandeur du certificat[115] (cf. *supra*). Par contre, si l'article 14, § 1er, point c), impose explicitement cette obligation de vérification de la complémentarité des données aux PSC qui les génèrent, il semble qu'il ne fasse pas peser la présomption de responsabilité sur les prestataires qui ne les génèrent pas. On pourrait en conclure que ladite présomption de responsabilité jouerait lorsque le PSC a généré lui-même les deux types de données alors qu'elle ne jouerait pas dans le cas contraire.

Cette discrimination de traitement ne se justifie pas, d'autant que la présomption de responsabilité consacrée par l'article 14 profite à une personne – celle qui se fie au certificat – qui est totalement étrangère au choix de la personne chargée de générer les données. Pourquoi la personne qui se fie à un certificat devrait-elle se limiter à constater que les données ne peuvent être utilisées de façon complémentaire pour engager la responsabilité du PSC lorsque ce dernier génère lui-même les données alors que, dans le cas où le PSC n'aurait pas généré les données, elle devrait faire positivement la preuve que le PSC n'a pas respecté son obligation prescrite à l'article 8, § 1er ?

Ainsi, nous pensons que la présomption de responsabilité existe également dans le cas où le PSC n'aurait pas généré les données. S'il est vrai qu'elle ne découle pas de l'article 14, § 1er, point c), on devrait pouvoir la déduire de deux autres dispositions. Premièrement, le point a) de l'article 14 crée aussi une présomption de responsabilité à charge du PSC quant à l'exactitude de toutes les informations contenues dans le certificat qualifié. Or l'annexe I relative aux informations contenues dans le certificat parle dans son point e), de données afférentes à la vérification de signature « qui correspondent » aux données pour la création de signature, sans faire de distinction si ces données sont générées par le PSC ou par l'utilisateur. On pourrait en déduire indirectement une obligation pour le PSC d'effectuer cette vérification, et une responsabilité sous-jacente qui découle du point a) de l'article 14. Deuxièmement, la disposition de l'article 8, § 1er, pourrait s'analyser, nous semble-t-il, en une obligation de résultat « allégée », dont la simple constatation de l'inexécution créerait une présomption de

[114] En raison probablement d'une erreur de plume, le texte utilise le terme « signataire », à l'instar de la directive, alors que cette loi emploie en principe la notion de « titulaire de certificat ».

[115] Cette précision n'existait par contre pas dans la directive, qui ne semblait envisager une obligation pour le PSC de vérifier la complémentarité des données que dans le cas où il les générait, ce qui a amené certains auteurs à critiquer cette réserve. Voy. M. ANTOINE et D. GOBERT, *J.T.D.E.*, *op.cit.*, p. 76 ; P. LECOCQ et B. VANBRABANT, *op.cit.*, p. 100, note 154 ; J.F. LEROUGE et Y. POULLET, *op.cit.*

responsabilité dans le chef du PSC. Toutefois, ce dernier devrait pouvoir se dégager de sa responsabilité en apportant simplement la preuve qu'il n'a commis aucune négligence. On n'exigerait donc pas qu'il doive se prévaloir d'une cause étrangère libératoire.

Enregistrement de la révocation du certificat – Le PSC peut voir sa responsabilité engagée dans l'hypothèse où il a « omis de faire enregistrer la révocation du certificat » (art. 14, § 2). Les mots « faire enregistrer » présentent, selon nous, une importance particulière. En effet, la présomption de responsabilité joue, non parce qu'il n'a pas révoqué le certificat, mais parce qu'il n'a pas procédé à l'enregistrement[116] alors que les conditions de la révocation étaient remplies. Dès lors, pour pouvoir bénéficier de la présomption de responsabilité de l'article 14, § 2, il nous semble que la personne qui se fie raisonnablement à un certificat devrait en premier lieu apporter la preuve que les conditions donnant naissance à l'obligation de révocation sont remplies. Cette preuve sera relativement aisée lorsque le titulaire a demandé la révocation, et dans cette hypothèse l'enregistrement de la révocation devait d'ailleurs être immédiate (art. 12, § 1er). Par contre, elle sera plus périlleuse pour les hypothèses visées à l'article 12, § 2 (cf. *supra*). A titre d'exemple, la personne qui se fie au certificat ne pourra pas reprocher au PSC de ne pas avoir fait « enregistrer la révocation » tant qu'elle n'aura pas prouvé que le PSC savait ou devait savoir qu'il existait des raisons sérieuses pour admettre que le certificat n'était plus conforme à la réalité ou qu'il avait été informé du décès du titulaire. Une fois cette preuve apportée, elle ne devra par contre pas apporter la preuve que le PSC a commis une faute du fait du non enregistrement de la révocation.

En vertu du régime mis en place, le PSC est responsable de tout préjudice causé à toute personne qui, en bon père de famille[117], se fie raisonnablement à un certificat lorsqu'un manquement à l'une des obligations énumérées ci-dessus est constaté. L'article 14, §§ 1er et 2, crée donc une présomption de responsabilité qui a pour effet de renverser la charge de la preuve : il suffit au bénéficiaire de cette présomption d'établir positivement son dommage et, pour le reste, la faute du PSC est présumée dans les hypothèses précitées. Cette présomption est toutefois réfragable : le PSC cesse d'être responsable s'il « prouve qu'il n'a commis aucune négligence ». Cette preuve ne sera pas facile à apporter : ce sera le cas s'il arrive à montrer qu'il a tout mis en œuvre en vue d'identifier le titulaire mais que les documents présentés étaient falsifiés et que de surcroît la falsification n'aurait pu apparaître qu'au terme d'un examen complexe par un expert. Par contre, il sera plus difficile de prouver qu'il n'a commis aucune négligence en cas d'omission d'enregistrer la révocation du certificat, sauf à se prévaloir d'un cas de force majeure.

Par ailleurs, la responsabilité du PSC ne peut être engagée dans les conditions de l'article 14 que pour autant que la personne se fie au certificat de manière « raisonnable » ou « en bon père de famille ». Si le PSC peut apporter la preuve que ce n'est pas le cas, il pourra se dégager de sa responsabilité notamment s'il prouve en plus qu'il n'a commis aucune négligence ou, à tout le moins, envisager un partage de responsabilité. En guise d'illustrations, on pourrait considérer qu'une personne ne se comporte pas raisonnablement ou en bon père de famille lorsqu'elle se fie à un certificat alors qu'elle ne vérifie pas la signature ou que le certificat n'est pas expiré ou révoqué pour chaque message reçu (cf. *supra*), savait ou devait

[116] C'est-à-dire à l'affichage dans l'annuaire électronique de la mention selon laquelle le certificat est révoqué.

[117] La loi n'utilise la notion de « bon père de famille » que dans le premier, et non le second, paragraphe de l'article 14. Ceci ne prête à notre avis pas à conséquence non seulement parce que cette notion n'existait pas dans la directive mais surtout parce qu'elle se rapproche en pratique du critère du « raisonnable ». Il s'agit dans les deux cas de critères abstraits, laissés à l'appréciation du juge, qui ont pour but de relativiser la responsabilité du PSC en fonction du comportement de la personne qui se fie au certificat.

savoir que le signataire est décédé ou a perdu la qualité spécifique indiquée dans le certificat, a été prévenue par le titulaire que ses données afférentes à la création de signature ont été divulguées à un tiers non autorisé ou qu'il a demandé au PSC de révoquer son certificat, n'a pas respecté les limites d'utilisation ou valeur maximale indiquée dans le certificat…

Le PSC peut, en outre, limiter sa responsabilité à l'égard des personnes qui se fient aux certificats qualifiés dans deux hypothèses. Le prestataire peut tout d'abord fixer des limites à l'utilisation du certificat[118] (art. 14, § 3). Il peut ensuite indiquer sur le certificat la valeur maximale des transactions pour lesquelles le certificat peut être utilisé (art. 14, § 4). Dans ces hypothèses, la loi indique sans équivoque que le PSC ne doit pas être tenu responsable du préjudice résultant soit de l'usage abusif – c'est-à-dire qui dépasse les limites fixées à son utilisation – soit du dépassement de la limite financière du certificat qui contient ce type de clause. La loi innove donc par rapport au droit commun en créant un mécanisme permettant au PSC de limiter sa responsabilité extracontractuelle.

Toutefois, les clauses limitatives de responsabilité ne sont opposables aux personnes qui se fient légitimement aux certificats que si celles-ci en ont pris connaissance ou, à tout le moins, ont pu raisonnablement en prendre connaissance au plus tard au moment de la consultation du certificat. C'est la raison pour laquelle elles doivent obligatoirement figurer *sur le certificat*[119]. *A contrario*, on en conclut que serait inopposable toute clause limitative de responsabilité du PSC, à l'égard des personnes qui se fient au certificat, indiquée à un autre endroit que sur le certificat[120], à tout le moins si elle n'est pas explicitement consentie par cette dernière. En sus, la loi exige que ces limites soient « discernables » par des tiers, critère qui sera apprécié au cas par cas par le juge. Toutefois, l'appréciation de ce critère constitue, selon nous, la seule marge de manœuvre du juge pour juger de l'opposabilité et de la validité des clauses limitatives de responsabilité. Cela revient donc à créer une obligation dans le chef de la personne qui se fie au certificat de prendre connaissance du contenu du certificat et d'en tirer les conséquences en cas de limitations y inscrites[121].

Le libellé des paragraphes 3 et 4 de l'article 14 donne l'impression que le PSC peut indiquer les limites susvisées sans devoir demander l'accord ni informer le titulaire de celles-ci et qu'en plus, ces limites ne profitent qu'au PSC, sans envisager la possibilité pour le titulaire du certificat de se prévaloir de ces limites à l'égard du destinataire du message. Cette impression est, à notre avis, trompeuse. En effet, la délivrance d'un certificat est avant tout le résultat d'une demande effectuée par un candidat-titulaire, qui doit garder la maîtrise de son contenu. Ainsi, toute limite d'utilisation ou valeur maximale indiquée dans le certificat doit être demandée ou, en tout cas, acceptée par le titulaire. Par contre, on pourrait, nous semble-t-il, admettre qu'un PSC refuse de délivrer un certificat au motif que le candidat titulaire n'accepte pas l'indication de ces limites dans le certificat[122,123]. Par ailleurs, on envisage mal que ces

[118] Il pourrait ainsi être indiqué que le certificat ne peut être utilisé que pour envoyer les déclarations TVA ou des documents uniquement à l'ONSS, ou encore des factures électroniques.

[119] Cette condition est clairement indiquée dans les §§ 3 et 4 de l'article 14 et est, elle-même, une condition pour que le certificat soit réputé qualifié (annexe I, i et j). Voy. aussi *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 37.

[120] Par exemple, des limites de responsabilités indiquées dans les « pratiques de certification » du PSC affichées sur son site web, encore même une mention du certificat renverrait-elle à la consultation du site.

[121] En ce sens, J.F. LEROUGE et Y. POULLET, *op.cit.*

[122] On peut d'ailleurs s'attende à ce que les politiques de tarification des PSC soient définies en fonction des risques, et donc des limites de responsabilité indiquées dans le certificat, qu'ils prennent en délivrant celui-ci.

[123] L'annexe II, point k), semble plaider en faveur du droit pour le PSC d'imposer « commercialement » les limites à l'utilisation du certificat en indiquant que le PSC est tenu « avant d'établir une relation contractuelle

limites ne puissent être opposées à l'égard de la personne qui se fie au certificat que par le PSC. Même s'il est vrai que les paragraphes 3 et 4 de l'article 14 ne visent pas textuellement cette hypothèse, un titulaire devrait malgré tout pouvoir se prévaloir de ces limites pour, si non s'exonérer, limiter sa responsabilité. En effet, commet une faute une personne qui se fie au certificat sans tenir compte des limites à son utilisation ou de la valeur maximale des transactions pour lesquelles le certificat peut être utilisé, d'autant que par hypothèse ses limites sont « discernables », faute qui est de nature à entraîner à tout le moins un partage de responsabilités avec le titulaire[124].

On devrait pouvoir admettre que les limites indiquées dans le certificat profitent au PSC, non seulement dans les hypothèses de responsabilité visées par les paragraphes 1 et 2 de l'article 14, mais également dans toutes autres hypothèses de responsabilité découlant d'une violation d'une de ses obligations consacrées par la loi (notamment de celles imposées à l'annexe II) ou d'une simple application du droit commun.

Une dernière question se pose : est-il possible pour le PSC d'indiquer dans le certificat d'autres clauses limitatives de responsabilité que celles visées dans les paragraphes 3 et 4 de l'article 14[125] ? D'après nous, plusieurs éléments confirment que rien ne s'y oppose. En premier lieu, la liste des mentions obligatoires de l'annexe I ne semble pas exclure l'indication d'autres informations. Ensuite, l'article 14 n'indique aucune restriction. Enfin, rappelons que le considérant 22 de la directive indique que « les PSC fournissant des services de certification au public sont soumis à la législation nationale en matière de responsabilité ». Dès lors, le droit commun de la responsabilité, qui permet ce type de limitations, trouve à s'appliquer.

Toutefois, pour que ces limites de responsabilité supplémentaires soient opposables, elles devraient à notre avis se trouver dans le certificat et être « discernables ». Elles devraient également respecter les règles de protection du consommateur et les limites jurisprudentielles classiques[126]. A ce propos, ces clauses ne pourraient pas avoir pour effet d'exonérer le PSC de ses obligations essentielles consacrées non seulement par les paragraphes 1 et 2 de l'article 14[127] mais aussi des obligations consacrées par les autres dispositions de la loi[128], sous réserve

---

avec une personne demandant un certificat à l'appui de sa signature électronique, [d']informer cette personne (…) des modalités et conditions précises d'utilisation des certificats, *y compris des limites imposées à leur utilisation* (…) ».

[124] Le titulaire pourrait difficilement invoquer une exonération totale de responsabilité dans la mesure où il commet également une faute en utilisant la signature et le certificat pour conclure une transaction qui ne rentre pas dans les limites d'utilisation du certificat ou qui dépasse la valeur maximale indiquée dans le certificat. Ce raisonnement s'impose, d'après nous, lorsque le titulaire est une personne physique (le titulaire est la personne qui signe matériellement). Par contre, les juridictions pourraient être plus souples lorsque le titulaire est une personne morale, dont on sait qu'elle se différencie de la personne qui utilisera en pratique la signature, en l'occurrence le représentant de la personne morale qui outrepasserait ses pouvoirs ! Nous renvoyons sur ce point à la contribution de Bernard Vanbrabant relative à la signature des personnes morales.

[125] On pense par exemple aux clauses classiques jouant sur le type de dommage réparable, de faute, sur les conditions d'engagement de la responsabilité (introduire l'action dans les deux semaines de la survenance du dommage par exemple), sur la distinction obligation de moyens et de résultat,…

[126] Voy. E. MONTERO, *op.cit.*, pp. 393-434.

[127] A cet égard, il est bon de rappeler que la version originaire du projet de loi consacrait un paragraphe, qui a toutefois disparu sans justification au cours des discutions parlementaires, dans l'article relatif à la responsabilité selon lequel « Toute convention contraire aux dispositions du présent article est réputée non écrite », paragraphe 4 de l'article 15 du projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques du 16 décembre 1999, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 37 et 78.

des limitations admises, notamment du plafond financier, en vertu des paragraphes 3 et 4 de l'article 14.

Rappelons que, selon nous, s'il est vrai que le PSC qui délivre des certificats qualifiés dans le cadre d'un réseau fermé *au sens large* ne devrait pas pouvoir déroger aux règles de responsabilité consacrées par l'article 14[129], cette possibilité pourrait être admise s'il les délivre dans le cadre d'un réseau fermé *au sens strict* (cf. *supra*). Par ailleurs, lorsque le PSC délivre des certificats dans le cadre d'un réseau fermé *au sens large*, il lui suffirait de ne pas indiquer dans les certificats qu'il émet la mention « certificat *qualifié* » pour échapper à la présomption de responsabilité mise en place par la loi.

e) L'arrêt des activités des prestataires (art. 15)

Dans le soucis d'assurer la pérennité des services offerts par des PSC délivrant des certificats qualifiés, l'article 15 envisage les obligations à charge de ces derniers lorsqu'ils cessent ou envisagent ce cesser leurs activités. Ces obligations varient en fonction du caractère volontaire (§ 1er) ou non (§ 2) de l'arrêt des activités.

Lorsqu'un PSC décide de mettre fin volontairement soit à l'ensemble de ses activités soit simplement à l'activité de délivrance de certificats *qualifiés*[130], il est tenu d'en informer l'Administration « dans un délai raisonnable ». Dans la mesure où cette information poursuit le double but d'éviter tout effet de surprise et de permettre à l'Administration de contrôler l'opération[131], nous ne décelons pas la raison qui justifie l'écoulement d'un délai, fût-il raisonnable, suite à la décision du PSC de mettre fin à ses activités. Dès lors, nous pensons que le « délai raisonnable » doit s'entendre comme un bref délai.

Au-delà de son devoir d'information, le PSC doit également s'assurer de la reprise de ses activités liées à la délivrance de certificats qualifiés par un autre PSC. Le cas échéant, ce dernier doit nécessairement garantir un même niveau de qualité et de sécurité que le PSC qui cesse ses activités[132]. Le texte de loi ne dit pas si cette garantie d'équivalence de qualité et de sécurité doit s'apprécier *in concreto* – en vérifiant que le PSC repreneur utilise les mêmes normes et procédures de qualité et de sécurité que le PSC cédant, spécialement si ces normes et procédures offrent un niveau de sécurité supérieur à celui exigé par la loi pour émettre des certificats qualifiés –, ou *in abstracto* – en se limitant à vérifier que le PSC repreneur remplit les conditions minimales prévues par la loi pour pouvoir émettre des certificats qualifiés, sans avoir égard au niveau de sécurité réellement atteint par le PSC cédant. En pratique, on peut s'attendre à ce que les PSC offrent, dans bien des cas, des niveaux de qualité de service et de sécurité supérieurs à ceux exigés par la loi et créent ainsi une concurrence sur le niveau de services offerts. Par ailleurs, l'utilisation de certificats qualifiés dans certains secteurs – notamment dans le domaine des services financiers – peut justifier un niveau de sécurité très

---

[128] A tout le moins, si le juge considère qu'il s'agit d'obligations essentielles. Jean-François Lerouge et Yves Poullet défendent l'idée selon laquelle toutes les obligations contenues dans la loi et ses annexes sont essentielles, *op.cit.*

[129] Partant, toute clause par laquelle le PSC renverserait la présomption de responsabilité mise en place par l'article 14 serait nulle.

[130] L'article 15, § 1er, utilise, non sans ambiguïté, les mots « activités de prestataire de service de certification qualifiée ».

[131] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 38.

[132] Le PSC « repreneur » sera également attentif au fait qu'il est soumis aux règles de responsabilité consacrées à l'article 14 pour les certificats qu'il reprend du PSC qui cesse ses activités (*cf. supra*).

élevé. Dans ce contexte, nous pensons qu'il est nécessaire d'apprécier *in concreto* la garantie d'équivalence du niveau de qualité et de sécurité pour éviter tout nivellement par le bas.

Si le PSC ne parvient pas à faire reprendre ses activités par un PSC garantissant un même niveau de qualité et de sécurité, il est tenu de révoquer les certificats. Il ne peut toutefois le faire que deux mois après en avoir averti les titulaires, ce qui contraint le PSC à continuer ses activités au moins pendant deux mois après avoir pris la décision de les cesser. Malgré la fin de ses activités, le PSC doit prendre les mesures nécessaires pour satisfaire à l'obligation prévue à l'annexe II, i), à savoir «enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile de 30 ans, en particulier pour pouvoir fournir une preuve de la certification en justice » (cf. *supra*). A cette fin, le PSC pourrait par exemple déposer les supports contenant ces informations auprès d'un autre PSC ou d'un notaire. Il devrait apporter selon nous la preuve à l'Administration de l'existencœ et du lieu du dépôt desdites informations afin que tout justiciable sache à qui s'adresser s'il souhaite les obtenir dans le cadre d'une procédure en justice 15 ou 30 ans après.

Il convient de préciser que le PSC qui arrête volontairement ses activités ne dispose pas du choix entre la reprise de celles-ci par un autre PSC ou la révocation des certificats. Il est tenu de tout mettre en œuvre en vue de procéder aux négociations nécessaires afin d'assurer la reprise de ses activités par un tiers[133]. Ce n'est qu'en cas d'échec qu'il devra révoquer les certificats délivrés par lui. Nous constatons néanmoins que le non respect de ces obligations, ainsi que le respect du caractère conditionnel de la seconde obligation, ne sont soumis à aucune sanction spécifique et adéquate[134]. Etant donné l'absence d'un pouvoir de contrainte consacré par la loi, on pourra donc difficilement empêcher un PSC de procéder directement à la révocation des certificats, sans avoir préalablement tenté de trouver un candidat repreneur.

L'article 15, § 2, vise l'hypothèse dans laquelle le PSC cesse ses activités pour « des raisons indépendantes de sa volonté ou en cas de faillite ». Dans ce cas, il est également tenu d'informer l'Administration. Par contre, il ne doit pas essayer, et ne semble d'ailleurs pas en avoir le droit, d'assurer la reprise de ses activités par un autre PSC garantissant un même niveau de qualité et de sécurité. Il doit directement « procéder à la révocation des certificats et prendre les mesures nécessaires pour satisfaire à l'obligation prévue à l'Annexe II, i)». Pourquoi cette différence de régime ? Probablement, le législateur pense que le caractère forcé de la cessation permet de craindre que dans les derniers mois de sa (sur)vie, le PSC n'était plus capable d'assurer correctement ses activités, et notamment de conserver un niveau de sécurité adéquat, ce qui justifierait une révocation obligatoire dans un soucis de prudence. Nous pensons que cette différence de régime ne se justifie pas pleinement. En effet, en cas de faillite d'un PSC par exemple, l'objectif premier du curateur consiste à valoriser au maximum les actifs de la société. Or, un certificat révoqué ne vaut plus rien ! N'aurait-il pas été plus intéressant de permettre au curateur de vérifier, avec l'aide éventuelle de l'Administration, si dans les faits le niveau de qualité et de sécurité généralement offert par le PSC a été atteint. Dans l'affirmative, le curateur devrait avoir le droit de ne pas révoquer les certificats et d'essayer de trouver un repreneur auquel il pourrait « vendre » les certificats. Une telle solution permettrait de satisfaire tant les titulaires de certificats, qui conservent ainsi leur

[133] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 38.

[134] La seule sanction prévue par l'article 20 consiste à « défendre au PSC de continuer à délivrer des certificats qualifiés ». Cette sanction ne devrait pas trop inquiéter le PSC qui décide volontairement de ne plus délivrer de certificats qualifiés ! Par contre, et à notre étonnement, les travaux parlementaires indiquent que « le PSC doit souscrire une assurance afin d'assurer soit la continuation du service à un niveau équivalent soit, à défaut, la révocation des certificats » ! Cette obligation ne semble néanmoins pas reprise dans le texte de loi.

certificat et ne doivent pas effectuer de nouvelle démarche auprès d'un nouveau PSC, que les actionnaires du PSC qui pourraient récupérer une partie de leur mise.

2. Les PSC accrédités

Comme vu précédemment, le principe posé par la loi, conformément à la directive européenne, est celui de la liberté de fourniture des services de certification (art. 4, § 2). En d'autres mots, cette dernière n'est soumise à aucune autorisation préalable. Toutefois, un tempérament vient quelque peu modérer le principe formulé.

En effet, selon l'article 3.2 de la directive, les Etats membres peuvent, tout en respectant le principe de la liberté d'exercice de l'activité de certification, instaurer ou maintenir des régimes *volontaires* d'accréditation visant à améliorer le niveau de service fourni[135]. Sur cette base, les articles 17 et 18 de la loi établissent un régime volontaire d'accréditation et offrent ainsi la possibilité à tout PSC de demander une accréditation à l'Administration, cette dernière étant en effet chargée, en vertu de l'article 18, 1°, d'octroyer et de retirer les accréditations.

Contrairement au premier projet de loi[136], la loi n'exige plus qu'un signataire obtienne un certificat d'un PSC *accrédité* pour pouvoir bénéficier de la clause d'assimilation visée à l'article 4, § 4. Cette solution avait été préconisée à l'époque pour des questions de sécurité juridique, notamment parce que les PSC accrédités faisaient l'objet d'un contrôle de conformité *a priori* grâce à l'audit effectué par l'entité[137]. Toutefois, la Commission européenne a informé la Belgique dans son avis circonstancié qu'elle ne pouvait lier la clause d'assimilation – en d'autres mots, la force probante des signatures électroniques – à l'accréditation des PSC[138]. Ce faisant, elle risquait de porter indirectement atteinte au principe de non autorisation préalable[139]. Le législateur belge a donc revu sa copie afin de tenir compte de cet avis.

L'octroi d'une accréditation est soumis à une double condition de fond (art. 17, § 1er, al. 1). D'une part, le PSC candidat à l'accréditation doit répondre aux exigences liées à la délivrance de certificats *qualifiés*, à savoir celles contenues dans les annexes I et II de la loi (cf. *supra*). Ensuite, le PSC doit également utiliser des dispositifs sécurisés de création de signature, c'est-

---

[135] Les critères d'accréditation doivent dans ce cas être « objectifs, transparents, proportionnés et non discriminatoires » (art. 3.2 de la directive européenne). En Belgique, le respect de ces critères semblait faire défaut dans le cadre du système d'accréditation mis en place par la Banque Carrefour de Sécurité Sociale. En effet, l'Arrêté Royal du 16 octobre 1998 ne soufflait mot ni de la procédure, ni des conditions relatives à l'accréditation (Arrêté Royal du 16 octobre 1998 « portant des dispositions relatives à la signature électronique, qui s'applique à la sécurité sociale, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *M.B.*, 7 novembre 1998, prolongé à plusieurs reprises). Il semble toutefois que cet Arrêté Royal, ainsi que l'accréditation mise en place par ce dernier, ne sont plus d'application car il n'a pas été prolongé. Sa dernière prolongation, qui résulte de l'Arrêté Royal du 13 juillet 2000 (*M.B.*, 4 octobre 2000), a expiré le 30 juin 2001 ! On présume que la Banque Carrefour de Sécurité Sociale a passé le relais à l'Administration mise en place par la loi du 9 juillet 2001.

[136] Projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques du 16 décembre 1999, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 68 à 81.

[137] Sur ce point, voy. *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 24 et 25.

[138] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 22.

[139] Sur ce débat, M. ANTOINE et D. GOBERT, *J.T.D.E.*, *op.cit.*, pp. 75-76 ; P. LECOCQ et B. VANBRABANT, *op.cit.*, pp. 91 et 119 à 121 ; D. GOBERT et E. MONTERO, « L'ouverture de la preuve littérale aux écrits sous forme électronique », *J.T.*, n° 6000, pp. 116-117.

à-dire ceux qui répondent aux exigences de l'annexe III[140]. En pratique, le contrôle de conformité du PSC aux exigences des annexes I, II et III est réalisé par une entité[141] (art. 17, § 1er, al. 2) qui, selon l'article 2, 13°, est un « organisme qui démontre sa compétence sur base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen »[142]. Pour éviter toute ambiguïté, il convient de préciser que les notions de certificat et d'accréditation visées par la loi du 20 juillet 1990 couvrent des réalités sensiblement différentes, et ne doivent pas être confondues avec celles proposées par la loi du 9 juillet 2001 ici commentée[143]. Sur la base du résultat de l'évaluation effectuée par ladite entité, l'Administration décide de l'octroi ou non de l'accréditation.

L'octroi de l'accréditation est également soumis à certaines conditions de forme ainsi qu'à des modalités financières, qu'il appartient au Roi de fixer en vertu de l'article 17, § 2. Ce dernier confie en effet le soin au Roi de préciser : la procédure de délivrance, de suspension et de retrait de l'accréditation (1°) ; les redevances dues au « Fonds pour l'accréditation » pour la délivrance, la gestion et la surveillance de l'accréditation (2°)[144] ; les délais d'examen de la demande (3°) ; et enfin, les modalités du contrôle des PSC accrédités (4°). Sur ce dernier point, on en conclut que l'Administration disposera probablement, pour le contrôle des PSC *accrédités*, de moyens supplémentaires à ceux déjà prévus par l'article 20[145].

En quoi une demande d'accréditation peut-elle présenter un intérêt pour un PSC puisque, comme dit précédemment, il n'est pas nécessaire de recourir aux services de PSC accrédités pour bénéficier de la clause d'assimilation ? Il suffit d'obtenir un certificat d'un PSC qui délivre des certificats *qualifiés*, et qui respecte l'ensemble des conditions pour ce faire. Le principal intérêt, à notre avis, réside dans l'atout commercial que peut représenter une accréditation. En effet, celle-ci sera probablement perçue par les utilisateurs comme un label de confiance, élément fondamental dans le développement des transactions en ligne. Par ailleurs, on peut s'attendre à ce qu'un PSC accrédité ait plus de facilités, en raison du contrôle préalable effectué dans le cadre de l'audit, à apporter la preuve d'une part, qu'il respecte effectivement les exigences des annexes, d'autre part, qu'il n'a commis aucune négligence, afin de se dégager des responsabilités qui lui incombent en vertu de l'article 14. Ensuite, il n'est pas improbable que le Roi impose, comme l'y autorise l'article 4, § 3, aux utilisateurs de signatures électroniques dans le secteur public d'obtenir un certificat auprès d'un PSC

---

[140] Cette obligation d'utilisation de dispositifs sécurisés de création de signature n'est consacrée expressément par la loi qu'à charge des PSC qui demandent une accréditation. Il semble néanmoins qu'elle existe également à charge du PSC qui délivre des certificats qualifiés sans accréditation, en vertu de son obligation d'être « suffisamment fiable pour fournir des services de certification » (annexe II, a).

[141] L'article 17, § 1er, al. 2, ajoute que l'entité est également tenue de vérifier la conformité du PSC, le cas échéant, aux exigences « liées à d'autres services et produits délivrés par les prestataires de service de certification ». Cette disposition vise probablement les exigences supplémentaires éventuelles auxquelles le Roi peut, en vertu de l'article 4, § 3, soumettre l'usage des signatures électroniques dans le secteur public. Sont-elles les seules ? La loi ne semble, en tous les cas, pas en envisager d'autres. Toutefois, peut-être le Roi peut-il déterminer d'autres exigences sur la base du paragraphe 2 de l'article 17 qui indique que « Le Roi précise les conditions visées au § 1er ». Le libellé et la portée de cette disposition ne sont cependant pas très clairs sur ce point.

[142] Pour des informations supplémentaires, généralement techniques, le lecteur consulte utilement le site du Ministère des affaires économiques : http://www.mineco.fgov.be/

[143] *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/2 du 10 novembre 2000, p. 19.

[144] On en conclut qu'un Fonds pour l'accréditation est institué et que l'accréditation est payante. Espérons que le montant des redevances ne sera pas de nature à dissuader les PSC à demander une accréditation!

[145] En ce sens, voy. également P. LECOCQ et B. VANBRABANT, *op.cit.*, pp. 91 et 103.

accrédité. Le cas échéant, on peut néanmoins s'attendre à ce que la Belgique s'attire une nouvelle fois les foudres de la Commission européenne… Enfin, l'accréditation peut présenter une véritable utilité pour les PSC établis en dehors de la Communauté (art. 16, § 2, cf. *infra*).

Pour terminer, précisons que la qualité de PSC accrédité est protégée pénalement. En effet, « sera puni d'une peine de huit jours à trois mois de prison et d'une amende de mille à dix mille francs, ou d'une de ces peines seulement, quiconque aura usurpé la qualité de prestataire de service de certification accrédité » (art. 21, § 1er). Par ailleurs, le juge « peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux »[146] aux frais de l'usurpateur (art. 21, § 2).

Section 4.
Le régime juridique des autres intervenants

Si les dispositions consacrées par la loi du 9 juillet intéressent, pour bonne part, les prestataires de service de certification, particulièrement ceux qui délivrent des certificats qualifiés, il ne faut pas oublier les quelques règles applicables aux autres intervenants dans l'utilisation de la signature électronique. L'article 3 confirme en effet que « La présente loi fixe (…) les règles à respecter par (…) les titulaires de certificats ». Nous nous intéressons également au rôle de contrôle de l'Administration ainsi qu'aux obligations des oubliés de la loi : les destinataires de messages signés électroniquement.

A. Les utilisateurs de certificat

Pour rappel, le législateur a pris la décision d'abandonner la notion « d'utilisateurs de certificats » pour consacrer celle de « titulaires de certificats » (cf. *supra*). L'article 19 précise expressément les obligations qui pèsent sur ces derniers. On relève que la loi ne semble pas restreindre ces obligations aux titulaires de certificats qualifiés mais vise les titulaires de tous types de certificats. Par contre, la loi ne souffle mot des éventuelles obligations qui sont à charge des autres utilisateurs de certificats, à savoir les destinataires de messages. Cela ne signifie toutefois pas que ceux-ci peuvent agir en toute liberté.

1. Les titulaires de certificat

Nous avons vu que le titulaire du certificat est « une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat » (cf. *supra*). L'article 19 consacre trois obligations à sa charge, libellées sous forme d'obligation positive mais aussi d'interdiction ou de responsabilité.

L'article 19, § 1er, indique que « le titulaire du certificat est seul responsable de la confidentialité des données afférentes à la création de signature ». Quelle est la portée de cette disposition ? Le titulaire ne pourrait en tout cas pas tenter de se dégager de sa responsabilité au motif par exemple que le détenteur n'a pas veillé à assurer le caractère secret des données.

[146] Une formulation plus large, à l'instar des articles 99 et 108 de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, était préférable dans la mesure où elle aurait également permis une insertion du jugement sur le site web du PSC et/ou un autre site web, probablement tout aussi efficace qu'une publication dans les journaux.

Il assume en effet « seul » cette responsabilité. Par ailleurs, le titulaire a, à tout le moins, une obligation de tout mettre en œuvre pour qu'un tiers non autorisé ne puisse pas prendre possession des données et les utiliser pour signer. Si le titulaire ne veille pas au respect de cette obligation, il doit faire révoquer le certificat dès qu'il a un doute quant au maintien de la confidentialité des données, notamment s'il constate que des actes ont été signés avec ses données par un tiers.

Doit-il assumer la paternité des actes signés frauduleusement par les tiers ? La réponse est certainement négative pour les actes signés après la révocation du certificat. Par contre, la réponse est moins évidente pour ceux signés avant la révocation. Certes, un signataire doit toujours pouvoir dénier sa signature – en vertu des articles 1323 et suivants du Code civil –, mais s'il le fait et s'il souhaite effectivement se dégager de l'acte signé litigieux, il devrait nous semble-t-il apporter la preuve que la perte de confidentialité des données n'est, non pas simplement le fait du non respect de son obligation ou de sa négligence, mais surtout le résultat d'une autre cause (un tiers a pu découvrir, par ingénierie inverse, les données afférentes à la création de signature à partir de celles afférentes à la vérification de signature, le PSC n'a pas assuré la confidentialité des données lors de la génération de celles-ci, un tiers a forcé le titulaire par la violence à divulguer les données, il prouve qu'il n'a jamais fait aucune demande d'un certificat auprès du PSC…)[147]. Cela revient en quelque sorte à créer une présomption réfragable selon laquelle toute utilisation des données afférentes à la création de signature est le fait de son titulaire. Dans le même temps, nous admettons qu'une telle présomption sera difficile à renverser[148]. S'il ne peut le faire, le titulaire serait en principe tenu par l'acte signé, et le destinataire du message devrait pouvoir engager sa responsabilité contractuelle[149]. Dans ce contexte, nous ne pouvons que conseiller aux titulaires de conserver leurs données afférentes à la création de signature sur un support sécurisé, dont l'accès est protégé par un moyen fiable (un mot de passe par exemple), et de conserver exclusivement le secret de ce moyen d'accès. Le titulaire peut également faire indiquer dans le certificat des limites à l'utilisation de ce dernier afin de réduire sa responsabilité face à ce risque.

Un bémol pourrait toutefois être apporté à la position ferme qui vient d'être défendue. En effet, on devrait pouvoir admettre qu'un titulaire puisse dénier, avec efficacité, sa signature et ainsi pouvoir se dégager de toute responsabilité contractuelle, tout en voyant sa responsabilité délictuelle engagée en raison du non respect de son obligation de maintien de la confidentialité de ses données (art. 19, § 1er). Ceci dit, étant donné la difficulté pratique de distinguer une première hypothèse, celle de l'acte litigieux réellement signé par un tiers suite à une négligence du titulaire, d'une seconde hypothèse, celle de l'acte litigieux signé par le titulaire mais dont il essaye de se dégager abusivement en invoquant qu'un tiers aurait réussi à obtenir les données qui devaient rester confidentielles, il nous paraît essentiel que le titulaire puisse apporter la preuve que l'acte a réellement été signé par un tiers (il arrive à identifier positivement le tiers qui a utilisé frauduleusement sa signature, il montre que l'objet de l'acte est tel qu'il n'est raisonnablement pas envisageable qu'il ait pu conclure pour son propre compte un tel acte…). Le cas échéant, le tiers qui subit un préjudice du fait du non respect par le titulaire de son obligation consacrée à l'article 19, § 1er, devrait être uniquement admis à engager la responsabilité du titulaire sur la base des articles 1382 et suivants du Code civil.

---

[147] Dans ces cas, ni la responsabilité contractuelle ni la responsabilité délictuelle du titulaire ne pourra être engagée.

[148] Voy. dans le même sens les commentaires du Conseil d'Etat sur l'avant-projet de loi, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 59 et 60.

[149] Sans préjudice de l'éventuelle responsabilité délictuelle.

Précisons que la responsabilité du titulaire de conserver la confidentialité des données afférentes à la création de signature ne débute que « dès le moment de la création » de ces données. Avant cela, rappelons que le PSC est tenu de garantir la confidentialité des données au cours du processus de leur génération (annexe II, g), pour autant bien évidemment qu'il génère lui-même les données. En pratique, toutefois, il sera extrêmement malaisé pour l'une ou l'autre des parties d'apporter la preuve que la divulgation de la clé privée, peut-être utilisée frauduleusement plusieurs mois après sa création, a eu lieu lors de sa génération par le PSC ou après sa prise de possession par le titulaire, et donc qu'elle résulte de la faute du PSC ou du titulaire[150]. On se trouve donc dans une hypothèse de responsabilité fautive chronologique dans laquelle le PSC et le titulaire risquent de se « renvoyer la balle ». Par ailleurs, on devrait pouvoir envisager une hypothèse de responsabilité partagée entre le titulaire et le PSC alors que l'on se trouve dans la période postérieure à la création des données. En effet, ce serait le cas si le titulaire n'a pas veillé à la confidentialité de ses données mais qu'en plus le PSC n'a pas révoqué le certificat alors qu'il existait des raisons sérieuses pour admettre que la confidentialité des données afférentes à la création de signature a été violée (art. 12, § 2, 1°).

Au-delà de cette obligation de confidentialité, le titulaire est également « tenu de faire révoquer le certificat en cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat » (art. 19, § 2). Cette obligation est logique : au risque de tromper les tiers et de ruiner l'économie du système, un titulaire ne peut plus se fonder sur un certificat dont le contenu ne correspond plus à la réalité, et doit donc le révoquer. Ce serait le cas notamment si une qualité spécifique venait à disparaître (un médecin est radié de l'ordre, par exemple). Par contre, il n'est pas certain que l'article 19, § 2, vise l'hypothèse du décès et qu'il crée une obligation à charge de la succession de procéder à la révocation du certificat. Néanmoins, celle-ci devrait au moins, nous semble-t-il, informer le PSC du décès du titulaire afin qu'il révoque le certificat en vertu de son obligation consacrée à l'article 12, § 2, 4°.

De plus, le titulaire doit aussi révoquer le certificat s'il a un doute quant au maintien de la confidentialité des données utilisées pour signer. Il suffit d'un doute. Aucune certitude dans son chef, ou l'existence de « raisons sérieuses » comme c'est le cas pour le PSC[151], ne sont exigées pour donner naissance à l'obligation. On devrait pouvoir considérer qu'un doute existe sur ce point, ou devrait exister dans le chef de tout titulaire, notamment lorsque le support contenant la clé privée est volé ou perdu. On constate que ce deuxième paragraphe de l'article 19 crée, à charge du titulaire, un obligation qui existe également, de manière moins intense il est vrai, dans le chef du PSC. Un partage de responsabilités est, une nouvelle fois, envisageable dans cette hypothèse.

Quelle sanction le titulaire encourt-il s'il ne respecte pas son obligation de révocation consacrée par l'article 19, § 2 ? La loi ne prévoit aucune sanction explicite. Le droit commun de la responsabilité contractuelle et extra-contractuelle devrait trouver à s'appliquer. Le destinataire de message notamment pourrait engager la responsabilité, contractuelle ou délictuelle suivant le cas, du titulaire. En effet, ce dernier commet une faute en ne révoquant pas un certificat alors qu'il a un doute quant au maintien de la confidentialité des données ou qu'il utilise un certificat dont il sait que les informations ne sont plus conformes à la réalité.

---

[150] Et pour complexifier la problématique, on constate que d'autres acteurs, tels que les concepteurs de dispositifs sécurisés de création de signature (annexe III, point a) et les organismes qui accréditent ces dispositifs en vertu de l'article 7, veillent aussi, de manière indirecte certes, au respect de cette confidentialité, et engagent leur responsabilité à cet égard.

[151] Article 12, § 1er, 1°.

Enfin, l'article 19, § 3, énonce une interdiction à charge du titulaire d'un certificat. En effet, « Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut, après l'expiration du certificat ou après révocation, utiliser les données afférentes à la création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de service de certification ». Un certificat possède une durée de vie limitée parce qu'on estime que les avancées technologiques sont telles qu'il est nécessaire, pour des raisons de sécurité, de renouveler régulièrement les produits de signature électronique, et notamment de générer un nouveau certificat avec de nouveaux outils technologiques lorsque le précédent arrive à échéance. La révocation d'un certificat est, quant à elle, généralement justifiée par des hypothèses qui permettent de présumer raisonnablement qu'il existe une faille de sécurité dans le système de certification (les données ne sont plus confidentielles, les informations ne sont plus conformes à la réalité, le PSC ne respecte pas ses obligations…).

Dans ces différents cas, il est donc logique d'interdire au titulaire d'utiliser des données afférentes à la création de signature qui correspondent à un certificat qui n'a plus aucune valeur. En pratique, il est impossible pour le PSC d'empêcher techniquement le titulaire d'utiliser ces données. Tout au plus, le PSC peut-il, et même doit-il, afficher de manière claire dans l'annuaire électronique la mention selon laquelle le certificat est expiré ou révoqué. Le destinataire d'un message pourrait (devrait), quant à lui, configurer son logiciel de vérification de signature de manière à ce qu'il vérifie systématiquement si le certificat est expiré ou révoqué, et le cas échéant, refuser le message signé[152]. Pour le reste, la loi se borne à consacrer juridiquement cette interdiction à charge du titulaire. Dans le même ordre d'idée, le titulaire ne peut pas non plus faire certifier ces données par un autre PSC. En effet, quel serait l'intérêt de demander la révocation d'un certificat parce qu'on craint qu'un tiers a pris frauduleusement possession des données afférentes à la création de signature si c'est pour aller faire certifier les données afférentes à la vérification de signature correspondantes auprès d'un autre PSC voire, selon nous, du même PSC ? On ferait naître à nouveau le risque de signature frauduleuse que l'on a voulu éviter en révoquant le précédent certificat ! Notons qu'il ne semble pas exister d'obligation pour le PSC de vérifier que les données offertes à la certification ont fait l'objet d'une certification préalable.

La loi ne prévoit aucune sanction en cas de non respect par le titulaire de ses obligations consacrées par le paragraphe 3 de l'article 19. Une nouvelle fois, le droit commun de la responsabilité contractuelle et/ou extra-contractuelle devrait s'appliquer. Par ailleurs, le titulaire pourrait éprouver certaines difficultés à contester la validité de sa signature en vertu des articles 1323 et suivants du Code civil si l'on peut prouver qu'il n'a pas respecté les obligations précitées.

2. Les destinataires de messages : un vide juridique ?

Dans le projet de loi déposé à la chambre le 16 décembre 1999, un article 21 consacrait les obligations que les destinataires de messages signés électroniquement étaient tenus de respecter[153]. Selon cet article, « Le destinataire d'un message signé électroniquement est tenu de vérifier la signature électronique au moyen des données afférentes à la vérification de signature et du certificat. Le destinataire vérifie également que le certificat n'est ni expiré ni

[152] En espérant que les logiciels actuels permettent ce type de configuration !

[153] Projet de loi relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques du 16 décembre 1999, *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, pp. 68 à 81.

révoqué ». Cet article, et par la même occasion les obligations à charge des destinataires, a mystérieusement disparu au cours des travaux parlementaires.

S'il est vrai que ces obligations ne sont plus expressément reprises par la loi, nous pensons qu'elles subsistent néanmoins indirectement et sont de nature à influencer tant la responsabilité des destinataires « à la hausse » que celle des titulaires ou du PSC « à la baisse ». En effet, un destinataire pourrait difficilement, s'il omet d'opérer systématiquement ces vérifications, engager la responsabilité contractuelle du titulaire pour un message envoyé après la révocation d'un certificat par exemple. Cela découle d'ailleurs de l'article 13, § 2, alinéa 2, selon lequel « La révocation est opposable aux tiers à partir de l'inscription » dans l'annuaire électronique de la mention selon laquelle le certificat est révoqué. Dans la même hypothèse, un destinataire ne devrait pas pouvoir reprocher au PSC que les informations contenues dans le certificat ne sont pas conformes à la réalité. En effet, on peut dégager de l'article 14, § 1er, une obligation à charge de toute personne qui se fie à un certificat de se comporter « en bon père de famille ». D'après nous, ne se comporte pas en bon père de famille un destinataire qui se fie à un document signé sans vérifier la signature[154] ou qui se fie à un certificat sans vérifier, chaque fois qu'un document signé est reçu, que ledit certificat n'est pas expiré ou révoqué. Il s'agit de normes de conduite raisonnables à appliquer en matière de signatures électroniques.

Il aurait été plus raisonnable de maintenir dans la loi ces obligations non seulement en vue de sauvegarder un juste équilibre entre les obligations des différentes intervenants (PSC - titulaire - destinataire de message) et les responsabilités qui en découlent mais en plus pour éviter tout effet de surprise à l'égard des destinataires de messages qui, en pratique, risquent de négliger ces opérations de vérifications systématiques. Notons d'ailleurs que l'article 11 de la loi type de la CNUDCI sur les signatures électroniques, relatif aux « Normes de conduite de la partie se fiant à la signature ou au certificat » envisage expressément le problème comme suit :

« Une partie se fiant à une signature ou à un certificat assume les conséquences juridiques découlant du fait qu'elle s'est abstenue :

a) *De prendre des mesures raisonnables pour vérifier la fiabilité d'une signature électronique ; ou*
b) *Si une signature électronique est étayée par un certificat, de prendre des mesures raisonnables pour : i) vérifier que le certificat est valide ou qu'il n'a pas été suspendu ou révoqué ; et ii) tenir compte de toute restriction dont le certificat ferait usage ».*

B. L'Administration

Nous avons vu précédemment que l'Administration joue un rôle prépondérant dans le cadre de l'accréditation volontaire des PSC. Sur ce point, nous présentons les rôles assignés par la loi à cette Administration ainsi que ses responsabilités connexes. De manière plus générale, l'Administration est également investie du contrôle de l'ensemble des PSC qui délivrent des certificats qualifiés, même si ces derniers ne sont pas accrédités.

[154] Contrairement à la signature manuscrite qui peut être vérifiée en un coup d'œil, la vérification d'un signature électronique nécessite quelques opérations techniques. Ce n'est d'ailleurs pas innocent si l'article 2, 8°, parle de « données afférentes à la vérification de signature », données « qui sont utilisées pour vérifier une signature électronique avancée ».

1. Responsable de l'accréditation et responsabilités connexes

Nous ne revenons pas sur les régimes volontaires d'accréditation, sur les conditions à remplir pour obtenir une accréditation ainsi que sur l'intérêt pour un PSC de demander celle-ci. Rappelons simplement que l'Administration est la cheville ouvrière du système d'accréditation mis en place par la loi. A cet égard, l'article 18 de la loi détermine les cinq missions essentielles qui lui sont attribuées.

Premièrement, l'Administration « octroie et retire les accréditations » (art. 18, 1°). On présume qu'elle est également chargée de la suspension éventuelle de l'accréditation puisque l'article 17, § 2, indique que le Roi précise la « procédure de délivrance, de *suspension* et de retrait de l'accréditation ». L'article 18 précise que « Cette mission s'exerce selon des règles, par des services et des personnes distincts de ceux visés à l'article 20, § 2 ». Il en résulte que le service au sein du Ministère des Affaires économiques qui s'occupe de l'octroi des accréditations doit être distinct de celui qui est chargé du contrôle des PSC qui délivrent des certificats qualifiés[155]. Le Roi devra tenir compte de cette contrainte lorsqu'il fixera la procédure d'accréditation en vertu de l'article 17 et les modalités de contrôle en vertu de l'article 20, § 2. Cette contrainte s'explique probablement par le souci d'assurer que, si le service a octroyé l'accréditation avec une certaine négligence, l'autre service qui effectue le contrôle puisse travailler sereinement et sanctionner toute anomalie éventuelle chez un PSC sans avoir l'impression de « se déjuger ».

Nous ne voyons pas l'intérêt de cette contrainte, d'autant que l'Administration chargée du contrôle l'est aussi pour celui des PSC accrédités. N'est-il pas judicieux de lier la procédure d'octroi et de retrait des accréditions et le contrôle du respect des conditions justifiant le maintien de l'accréditation ?

Pour prendre sa décision d'octroyer ou non l'accréditation, rappelons que l'Administration s'adjoindra l'aide d'une entité (cf. *supra*). Sur ce point, et c'est la deuxième mission confiée à l'Administration, celle-ci « supervise les procédures d'audit des entités visées à l'article 2, 13°) ainsi que les activités de ces entités dans le cadre des procédures d'accréditation » (art. 18, 3°).

Troisièmement, l'Administration est chargée de « coordonner l'application cohérente et transparente des principes et procédures d'accréditation en application de la présente loi » (art. 18, 2°).

Les deux dernières missions de l'Administration visent à assurer la transparence et la circulation de l'information. En effet, elle doit « communiquer à la Commission et aux Etats de l'Espace économique européen : a) les informations sur le régime volontaire d'accréditation instauré en application de la loi ; b) les nom et adresse de tous les prestataires de service de certification accrédités dans ce cadre » (art. 18, 4°). Elle doit également « exécuter l'ensemble des notifications visées à l'article 11 de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques » (art. 18, 5°). En vertu de cet article 11, l'Administration est tenue, au-delà des informations visées à l'article 18, 4°, de communiquer, d'une part, les exigences supplémentaires éventuelles pour l'utilisation des signatures électroniques dans le secteur

[155] Rapport fait au nom de la Commission de l'économie, de la politique scientifique, de l'éducation, des institutions scientifiques et culturelles nationales, des classes moyennes et de l'agriculture, *Doc. parl.*, Ch. repr., sess. ord. 2000-2001, n° 322/3 du 5 février 2001, p. 10.

public que le Roi aurait prises en application de l'article 4, § 3, de la loi, d'autre part, ses propres nom et adresse en qualité d'organisme responsable de l'accréditation et du contrôle. Rappelons que l'Administration communiquera aussi les coordonnées des organismes visés à l'article 7, § 2, de la loi. Enfin, l'Administration n'oubliera pas de communiquer tout changement éventuel de ces informations « dans les meilleurs délais » (art. 11.2 de la directive).

2. Responsable du contrôle et sanctions

Le principe consacré par la loi étant que tout PSC peut délivre des certificats *qualifiés* indépendamment de tout contrôle ou autorisation préalables, il était important de mettre en place un contrôle *a posteriori* efficace. L'article 20 charge en effet l'Administration du contrôle des PSC « qui délivrent des certificats qualifiés au public »[156].

L'article 20, § 1er, laisse même supposer, par la largesse de son libellé, que l'Administration est en droit d'exercer son contrôle à l'égard de tous les PSC, y compris ceux qui ne délivrent pas de certificats qualifiés. Le cas échéant, le contrôle sera en pratique relativement restreint dans la mesure où il ne portera que sur le respect des dispositions relatives à la protection des données à caractère personnel (art. 5), contrôle pour lequel la Commission de protection de la vie privée est également compétente. Par contre, l'Administration est l'organe le mieux placé pour « traquer » les PSC, encore même ne délivreraient-ils pas de certificats qualifiés, qui usurperaient la qualité de PSC accrédité et transmettre, si nécessaire, l'information aux autorités judiciaires qui pourront agir conformément à l'article 21.

La loi ne s'étend pas sur les moyens de contrôle dont dispose l'Administration pour exercer efficacement sa tâche. Elle confie en effet le soin au Roi de « déterminer, par arrêté délibéré en Conseil des Ministres, les règles relatives au contrôle des prestataires de service de certification ainsi que les moyens de droit dont l'Administration peut se prévaloir » (art. 20, § 1er). Elle ajoute que « Sous certaines conditions, fixées par le Roi, l'Administration est habilitée à demander aux prestataires de service de certification, toutes les informations nécessaires à la vérification de l'observation, par ceux-ci, de la présente loi » (art. 20, § 2). Tant que ces arrêtés royaux d'exécution ne sont pas pris, l'Administration est dépourvue de tout moyen de contrôle… alors que les PSC peuvent émettre librement des certificats qualifiés depuis l'entrée en vigueur de la loi !

Si le Roi n'a pas encore déterminé les moyens mis à la disposition de l'Administration pour exercer son contrôle, la loi indique par contre les moyens d'action dont elle dispose lorsqu'elle constate qu'un PSC qui délivre des certificats qualifiés – pour autant qu'il soit établi en Belgique[157] – n'observe pas les prescriptions de la loi. Dans ce cas, l'Administration « le met en demeure[158] et fixe un délai raisonnable endéans lequel le prestataire de service de certification doit avoir pris les mesures nécessaires afin d'agir à nouveau en conformité avec la loi » (art. 20, § 3).

---

[156] Les mots « au public » prêtent à confusion. Cela signifie-t-il que l'Administration ne peut exercer son pouvoir de contrôle à l'égard des PSC qui délivrent des certificats qualifiés exclusivement dans le cadre d'intranet par exemple ? Ni la loi ni les travaux parlementaires ne donnent d'éléments de réponse à cette question. Il nous semble que dans le cadre d'un réseau fermé au sens strict (cf. *supra*), l'Administration ne peut exercer son pouvoir de contrôle.

[157] Cette disposition fait écho à l'article 3.3. de la directive selon laquelle « Chaque Etat membre veille à instaurer un système adéquat permettant de contrôler les prestataires de service de certification établis sur son territoire et délivrant des certificats qualifiés au public ».

[158] Et non en défaut comme il est indiqué, suite probablement à une erreur matérielle, dans la loi.

Si le PSC ne prend pas les mesures nécessaires dans ce délai raisonnable, fixé discrétionnairement par l'Administration en fonction du cas d'espèce[159], afin de régulariser la situation, celle-ci doit saisir les tribunaux pour qu'ils prennent deux types de mesures[160,161]. D'une part, les tribunaux défendent au PSC de continuer à délivrer des certificats qualifiés. D'autre part, ils enjoignent au PSC d'informer immédiatement les titulaires des certificats qualifiés, délivrés par lui, de leur non-conformité aux prescriptions de la loi du 9 juillet 2001 (art. 20, § 4). Rappelons que dans ce cas, le PSC est en outre tenu de révoquer tous les certificats qualifiés en application de l'article 12, § 2, 2°.

Si le PSC est accrédité, l'Administration doit en plus procéder au retrait d'office de son accréditation[162]. Le PSC est alors tenu de mentionner dans son annuaire électronique le retrait de l'accréditation et d'en informer sans délai les titulaires de certificats (art. 20, § 5).

Section 5.
La reconnaissance transfrontière des certificats qualifiés

Afin de revêtir une réelle utilité dans le cadre du développement du commerce électronique sans frontière, toute infrastructure de certification doit être envisagée dans une perspective internationale. L'article 16 de la loi, qui traite des certificats délivrés à titre de certificats qualifiés par des PSC étrangers, fait écho à cette préoccupation. Dans ses deux paragraphes, l'article précité établit clairement une distinction entre les certificats qualifiés délivrés à l'intention du public[163] par un PSC qui est établi dans un Etat membre de l'Espace économique européen (§ 1er) et ceux délivrés à titre de certificats qualifiés à l'intention du public par un PSC établi dans un pays tiers – c'est-à-dire non membre de l'EEE (§ 2).

Pour les premiers, l'article 16, § 1er, les assimile aux certificats qualifiés délivrés par un PSC établi en Belgique. En d'autres mots, ils peuvent bénéficier en Belgique des mêmes effets juridiques que ceux reconnus aux certificats qualifiés « belges », notamment ceux qui découlent de la clause d'assimilation consacrée par l'article 4, § 4, de la loi[164]. La loi étant le résultat de la transposition d'une directive visant à harmoniser les règles nationales, le principe d'assimilation ne constitue finalement que le corollaire du principe de reconnaissance mutuelle qui découle de l'harmonisation, le tout contribuant à assurer la libre prestation des services de certification. Ce principe d'assimilation pourra néanmoins poser des problèmes en raison du caractère minimal de l'harmonisation. A titre d'exemple, un juge belge doit-il octroyer à un certificat « non belge » les effets juridiques de l'article 4, § 4, alors qu'il constate que l'une des hypothèses de révocation prévue par la loi belge était remplie et aurait

[159] *Doc. parl.*, Ch. repr., sess. ord. 1999-2000, n° 322/1 du 16 décembre 1999, p. 41.

[160] La formulation de la disposition plaide en faveur d'une obligation plutôt que d'une possibilité donnée à l'Administration. En sens contraire, voy. P. LECOCQ et B. VANBRABANT, *op.cit.*, p. 103.

[161] Comme le souligne P. LECOCQ et B. VANBRABANT, « On peut s'étonner qu'une modification du Code judiciaire n'ait pas été envisagée pour donner au Président du tribunal de commerce, statuant comme en référé, la compétence spéciale de connaître cette action », *op.cit.*, p. 103.

[162] Une nouvelle fois, il s'agit d'une obligation pour l'Administration. En sens contraire, voy. P. LECOCQ et B. VANBRABANT, *op.cit.*, p. 103.

[163] Nous ne voyons pas pourquoi les principes d'assimilation et d'équivalence consacrés par l'article 16 ne devraient profiter qu'aux certificats qualifiés délivrés « à l'intention du public », à l'exclusion par exemple des certificats qualifiés délivrés dans le cadre d'un intranet. Cependant, il est vrai qu'en pratique, la question ne se posera probablement pas souvent.

[164] Pour autant bien entendu que les autres conditions requises par l'article 4, § 4, soient remplies.

obligé un PSC belge à procéder à cette révocation, hypothèse toutefois non visée par la loi du PSC non belge, ce qui explique la subsistance dudit certificat ?

Pour les seconds par contre, l'article 16, § 2, prévoit qu'ils ne sont reconnus équivalents, sur le plan juridique, aux certificats délivrés par un PSC établi en Belgique que si l'une au moins des trois hypothèses suivantes est satisfaite.

Soit le PSC étranger est accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un Etat membre de l'EEE[165]. Si le PSC étranger demande une accréditation[166], il devra nécessairement se conformer à la réglementation nationale, qui transpose la directive européenne, de l'Etat membre en question et ses activités seront soumises au contrôle de l'Administration de ce même Etat[167] (art. 16, § 2, 1°).

Soit un PSC établi dans la « Communauté européenne »[168] garantit le certificat délivré à titre de certificat qualifié par le PSC étranger, pour autant que le premier PSC satisfasse à sa réglementation nationale qui transpose la directive européenne (art. 16, § 2, 2°). Même si le texte ne le précise pas, nous pensons que le PSC établi dans la Communauté européenne doit lui-même délivrer des certificats qualifiés et respecter l'ensemble des exigences de sa loi nationale relatives à la délivrance desdits certificats[169]. Pour le reste, la loi ne précise pas les modalités techniques par lesquelles le PSC va garantir les certificats. On en conclut que les PSC sont libres à cet égard. Rappelons qu'une telle garantie n'est pas sans risque. En effet, l'article 14 indique sans équivoque que le PSC assume pour les certificats qu'il garantit les mêmes responsabilités que celles qu'il assume pour ses propres certificats qualifiés.

Soit le certificat étranger ou le PSC étranger est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté européenne et des pays tiers ou des organisations internationales (art. 16, § 2, 3°)[170].

Nous pensons que cet article 16 – qui crée une espèce d'interopérabilité juridique – restera lettre morte tant qu'il n'existera pas une véritable interopérabilité technique entre les différents prestataires de service de certification. S'il est vrai que le considérant numéro 5 de la directive européenne souligne qu'il « convient de promouvoir l'interopérabilité des produits de signature électronique », il n'existe, à notre connaissance aucune obligation explicite à charge des opérateurs de veiller à cette interopérabilité lors de l'émission de certificats qualifiés.

---

[165] En raison de l'harmonisation et de la reconnaissance mutuelle qui en découle, le PSC étranger ne doit donc pas nécessairement être accrédité en Belgique.

[166] Il s'agit d'un intérêt supplémentaire à la mise en place d'un système d'accréditation (cf. *supra*).

[167] Le lecteur attentif constatera que le point a) du paragraphe 2 de l'article 16 est une transposition incorrecte de l'article 7, 1, a), de la directive. De surcroît, ce point n'a aucun sens : comment un PSC étranger pourrait-il respecter « *sa* réglementation nationale qui transpose la directive européenne » puisque, par principe, la directive n'a pas été et ne devait pas être transposée dans le pays étranger en question !

[168] Nous ne comprenons pas pourquoi cette deuxième hypothèse est limitée aux PSC établis dans la Communauté européenne et ne s'applique pas à l'ensemble des PSC établis dans un Etat membre de l'EEE. En effet, les Etats membres de l'EEE sont en principe destinataires de la directive européenne, comme le confirme d'ailleurs le paragraphe 1er de l'article 16. Nous pensons qu'il s'agit probablement d'une erreur de plume.

[169] En effet, si on fait une application servile du texte, un PSC qui ne délivre pas de certificats qualifiés respecterait « sa réglementation nationale » s'il se limite à faire application des règles relatives à la vie privée. Or, on conçoit mal que ce PSC puisse garantir des certificats qualifiés délivrés par un PSC étranger !

[170] La Commission peut, en vertu de l'article 7.2. de la directive, être chargée de négocier de tels accords, après avoir obtenu du Conseil un mandat à cette fin.

Conclusion

L'utilisation de la signature électronique et la prestation de services de certification devaient-elles être encadrées légalement ? Nous le pensons. Nous concluions déjà dans un article en 1998 avec Mireille Antoine sur la nécessité de mettre en place les bases légales adéquates afin d'assurer la reconnaissance juridique des signatures électroniques et d'offrir un maximum de souplesse tout en maintenant un niveau de sécurité et de confiance élevé dans les services de certification[171]. C'est désormais chose faite puisque depuis le 9 octobre 2001, la loi du 9 juillet 2001, fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification, est entrée en vigueur.

A quelques exceptions ou nuances près, les grandes lignes de la conclusion de notre article rédigé en 1998 peuvent être reprises ici. Nous estimions en effet que la « réglementation sur la certification » devait présenter un certain nombre de points. La plupart d'entre eux sont désormais consacrés par la loi du 9 juillet 2001.

La loi consacre certains principes de base tels que le droit pour toute personne de continuer à utiliser sa signature manuscrite, encore que les termes utilisés par la loi sont malheureusement plus ambigus, ainsi que celui de choisir le PSC (accrédité) auquel elle compte s'adresser en vue d'obtenir un certificat. Par contre, et suite aux injonctions adressées par la Commission européenne, la loi ne lie plus le caractère qualifié du certificat à l'accréditation du PSC qui les délivre : si un système d'accréditation est mis en place, celui-ci doit nécessairement être volontaire, et aucune mesure ne peut avoir pour effet d'inciter indirectement les PSC à demander une accréditation.

Une réglementation de la certification doit également, à l'instar de celle qui est relative à la signature, demeurer ouverte aux développements technologiques. Cette ouverture est assurée par le principe de neutralité technologique adopté, neutralité qui apparaît clairement dans les termes utilisés pour définir les concepts de la loi (signature électronique avancée, données afférentes à la création ou à la vérification de signature, dispositifs de création de signature…). On reconnaîtra néanmoins que l'analyse de ces définitions a démontré que certaines difficultés ou zones d'ombre subsistent : pourquoi avoir maintenu le terme « signataire » dans certaines dispositions de la loi alors que la liste de définitions de celle-ci ne vise à dessein que le titulaire du certificat ; les notions de données afférentes à la création ou à la vérification de signature permettront-elles en pratique d'englober d'autres mécanismes de signature que ceux bien connus de clés privées et publiques ; le caractère unique apparaissant dans la définition de données afférentes à la création de signature crée-t-il une obligation à charge du PSC de vérifier systématiquement l'unicité de ces données avant de délivrer un certificat ; quand pourra-t-on véritablement considérer qu'un dispositif de création de signature est sécurisé ; une interprétation stricte de la notion de PSC ne risque-t-elle pas d'étendre le champ d'application de la loi à des hypothèses non prévues par les auteurs du texte ; etc. On le voit, les questions sont encore nombreuses. Certes, nous avons essayé d'y apporter des réponses mais seule une période de rodage de cette loi permettra d'apprécier la pertinence de ces ébauches de solutions.

Nous nous sommes également interrogé sur le champ d'application de la loi et sur le caractère impératif de ses dispositions. Nous avons tenté de mettre de l'ordre dans les notions de

[171] M. ANTOINE et D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.*, juillet-octobre 1998, n° 4/5, pp. 285 à 310.

réseaux ouvertes et fermés, et pour ces derniers proposés une distinction entre réseau fermé *au sens strict* et *au sens large*. Cette distinction devrait aider à déterminer le caractère impératif ou non des dispositions de la loi.

Pour le reste, la réglementation relative à la certification doit essentiellement fixer les droits et obligations des différents acteurs, à savoir les PSC d'un coté et les utilisateurs de certificats de l'autre.

En ce qui concerne les obligations incombant aux PSC, elles sont surtout conditionnées par la nature particulière des activités exercées. Dans le cadre de réseaux ouverts, la signature est appelée à jouer seule la fonction d'identification alors que dans le cadre contractuel traditionnel, la signature n'était guère l'élément le plus important, ni même l'élément déterminant dans l'identification du cocontractant. Les PSC se voient donc reconnaître une mission spécifique qui transcende largement l'activité de renseignement. Il apparaissait, dès lors, indispensable que l'étendue de leurs obligations soit clairement définie par la loi, spécialement lorsqu'ils délivrent des certificats qualifiés dont on sait qu'ils permettent de bénéficier de la clause d'assimilation à la signature manuscrite.

Le PSC doit accomplir les missions fondamentales qui lui sont imposées par la loi. Il doit respecter les nombreuses exigences relatives aux certificats qualifiés, visant essentiellement à garantir la sécurité et la transparence des services de certification. Il doit également assumer les responsabilités liées aux spécificités de ses activités, particulièrement la présomption de responsabilité consacrée à l'article 14, et demeurer l'interlocuteur privilégié en cas de litige relatif à un certificat émis sous son autorité. Le cas échéant, le PSC est tenu d'opérer la révocation des certificats dans les limites tracées par la loi. Enfin, le PSC ne peut mettre fin à ses activités sans avoir accompli certaines démarches préalables précisées dans la loi. Nous avons montré à suffisance que certaines de ces obligations méritaient de sérieux éclaircissements et des précisions sur leur portée.

D'une manière générale, le PSC est tenu de respecter le droit commun de la vie privée lors de la collecte des données ainsi que les deux règles spécifiques consacrées par la loi. Le titulaire peut, s'il le souhaite et à certaines conditions, demander à garder l'anonymat et obtenir un certificat avec un pseudonyme.

Diverses obligations pèsent également sur les utilisateurs de certificat. En effet, le titulaire de certificat est tenu de fournir des informations exactes au PSC et de l'informer de tout changement de ces dernières, de préserver la confidentialité de ses données afférentes à la création de signature et, le cas échéant, de faire procéder à la révocation du certificat. Le destinataire d'un message signé électroniquement n'est, quant à lui, pas directement visé par la loi. Néanmoins, nous avons pu déduire de certaines dispositions que celui-ci est tenu de vérifier la signature au moyen du certificat correspondant et de s'assurer que celui-ci n'est pas expiré ou révoqué.

Enfin, nous avons montré que, en déterminant les conditions permettant d'assurer une « interopérabilité juridique » entre les certificats qualifiés, la loi n'a pas oublié le caractère de plus en plus international des relations commerciales.

Une autre question se pose : l'utilisation de la signature électronique et la prestation de services de certification auraient-elles dû être encadrées *autrement* ? Probablement pas. Certes, la loi n'est pas un exemple de perfection mais il faut reconnaître que faire œuvre

législative dans un domaine nouveau et à ce point technique n'est pas un exercice facile. Espérons qu'une période de rodage de la loi ainsi que la créativité des juges et des praticiens permettront d'éclaircir les nombreuses imprécisions qui subsistent ainsi que certaines zones d'ombre. Toutefois, cette période de rodage ne pourra réellement commencer que lorsque les arrêtés royaux d'exécution de la loi ainsi que les normes techniques visées à l'article 6 seront adoptés… ce que nous attendions toujours au moment de la rédaction de ces lignes !

Didier GOBERT
Assistant au CRID (Université de Namur)
Consultant en droit de l'informatique (www.consultandtraining.com)

Publié *in La preuve*, Formation permanente CUP, Volume 54, mars 2002, pp. 83 à 172.

Table des matières