

Le décret du 30 mars 2001 relatif à la signature électronique: lecture critique, technique et juridique*

Isabelle de Lamberterie

Directeur de recherche au CNRS-CECOJI (UMR 65-67), antenne parisienne.

Jean-François Blanchette

Doctorant au Département d'études des sciences et des technologies, Institut Polytechnique de Rensselaer, USA, et chercheur invité au CNRS-CECOJI.

Résumé: *Avec la publication du décret du 30 mars 2001, la signature électronique sécurisée fait dorénavant partie du paysage juridique français. Dans cet article, nous nous attachons à présenter aussi pédagogiquement que possible ce texte très technique, ainsi que le contexte normatif auquel il se rattache. Nous dégageons également la façon dont le texte articule les différentes procédures relatives à la signature — certification, création et vérification. Enfin, nous mettons en relief les questions que soulèvent l'effectivité de ces procédures, en particulier celles qui touchent à la pérennité des documents signés.*

Le développement rapide de la société de l'information est l'occasion d'un déploiement important de mesures techniques visant à rencontrer les exigences de sécurité juridique d'une telle société. Conscients des risques induits par des échanges non sécurisés au sein des réseaux électroniques, et désireux de stimuler la confiance dans le commerce électronique, les pouvoirs publics ont graduellement mis en place les conditions de mise en œuvre de la signature électronique.

Trois dates marquent — à ce jour — les **premiers contours** du cadre juridique de la signature électronique:

- le 13 décembre 1999, avec la publication de la directive européenne «¹ sur un cadre communautaire pour les signatures électroniques¹»;
- le 13 mars 2000, avec la loi « portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique² »;

* *La Semaine Juridique, Editions Affaires et Entreprises*, no. 30, 1269-1275 (juillet 2001).

¹ Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, JOCE du 19 janvier 2000, L 13, p. 12.

— le 30 mars 2001, avec l'adoption du décret «*pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique*»³».

Il s'agit de premiers contours: ces textes, tout en définissant un cadre normatif, laissent ouvertes les possibilités d'adaptation et d'évolution des techniques. En effet, ils sont le fruit d'une longue négociation entre des objectifs apparemment contradictoires: il s'agissait, d'une part, de répondre aux besoins de sécurité qu'engendre le commerce électronique et les échanges à travers des réseaux ouverts, et, d'autre part, de ne pas enfermer le cadre normatif dans un carcan technique qui, s'il répond aujourd'hui à un certain type de besoins, pouvait, dans un avenir plus ou moins proche, s'avérer inadapté à d'autres finalités.

Ainsi, en définissant l'écrit et la signature indépendamment d'un support ou d'une technique, le législateur français a laissé ouverte la possibilité de reconnaître la valeur probatoire de différents supports et différentes techniques. C'est ce même esprit qui préside aujourd'hui à la réflexion internationale sur ces questions, à la CNUDCI par exemple, où la préparation de la future loi modèle sur la signature électronique prend en compte la diversité des techniques de signature électronique⁴.

C'est en s'inscrivant dans une démarche similaire que nous proposons une lecture du décret du 31 mars, décret qui poursuit la transposition en droit français de la directive européenne du 13 décembre 1999. Notre approche, de par la formation des auteurs, sera à la fois technique et juridique. Elle se voudrait, aussi, descriptive et prospective.

Il s'agit en effet de relever les risques de confusion ou d'amalgame qui découleraient d'une interprétation superficielle des textes (et de certains commentaires qui les accompagnent) entre, d'une part, signature électronique et, d'autre part, certains procédés de signature utilisant la cryptographie. La question de la **fiabilité** de la signature électronique et par conséquent, la garantie de l'**intégrité** des documents signés, seront nos fils conducteurs. On étudiera d'une part comment peut être

² *Loi 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JO du 14 mars 2000, p. 3968.*

³ *Décret no. 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, JO du 31 mars 2001, p. 5070.*

⁴ *Projet de loi type de la CNUDCI sur les signatures électroniques et guide pour son incorporation, A/CN.9/WG.IV/WP.88, 30 janvier 2001.*

appréhendée la notion de signature électronique (I), et d'autre part, les exigences que le droit impose pour présumer sa fiabilité (II).

I- La notion de signature électronique

Le décret définit la signature électronique comme «*une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies par la première phrase du second alinéa de l'article 1316-4 du code civil*»⁵. C'est donc dans la loi du 13 mars 2000 qu'il faut chercher les éléments permettant de cerner le cadre juridique de la signature électronique. La loi fournit une définition de la signature, que celle-ci soit ou non électronique (A). Elle indique aussi à quelles conditions la signature électronique peut être une signature efficace (B). Enfin elle pose le principe d'une présomption de fiabilité quand la signature électronique est sécurisée (C).

(A) Définition de la signature

Avant le vote de la loi du 13 mars 2000, la signature est entendue comme un écrit de la main de celui qui s'engage⁶.

On pourrait penser que, pour la preuve des actes, la loi du 13 mars 2000 remet en cause ce principe. Il n'en est rien, car la loi ne fait aucune référence à une forme quelconque de la signature, et c'est uniquement sa fonction qui est prise en compte. En donnant une définition fonctionnelle de la signature, le législateur applique une démarche identique à celle qui a été choisie pour définir l'écrit.

En effet, le législateur reconnaît la valeur probatoire de l'écrit électronique — au même titre que l'écrit sur support papier — «*sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité*»⁷.

Si la forme est indifférente, l'écrit, comme la signature, n'échappe pas au besoin d'une formalisation quelconque, et il ne peut y avoir signature sans signe. Dans la mesure où ce signe, quelqu'il soit, est doté d'une signification intelligible, il est un écrit au sens du nouvel article 1316 du code civil, c'est à dire «*... une suite de lettres, de caractères, de chiffres*

⁵ Art.1.

⁶ I. Dauriac, *La signature*, thèse de doctorat, Université Panthéon-Assas (Paris II), 1997, no. 102 et s.

⁷ C. civil, art. 1316-1.

ou de tous autres signes ou symboles, dotés d'une signification intelligible quels que soient leur support et leurs modalités de transmission»⁸.

La signification de l'écrit qu'est la signature est posée par l'article 1316-4: «*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. ...*»⁹.

Ainsi, la signature est un écrit apposé sur un acte, qui permet à un lecteur d'identifier le signataire de cet acte (1) et d'en inférer la manifestation de son consentement à cet acte (2). Encore faut-il que cet écrit soit intelligible: la signature doit pouvoir être lue et correctement interprétée. Cette dernière (et difficile) question sera approfondie plus loin, lors de l'analyse critique des signatures électroniques sécurisées.

(1) L'identification du signataire

L'identification du signataire passe par un signe, qui, comme le remarque Isabelle Dauriac, doit émaner du signataire et être distinctif¹⁰. D'une part, ce signe permet au signataire de se faire connaître, et d'autre part, il lui permet d'être reconnu. Cette reconnaissance est fonction de la capacité de celui qui aura à interpréter ce signe et à en tirer les conséquences. Bien entendu, l'identification ne passe pas obligatoirement par le nom et le prénom: tout autre signe remplissant les conditions ci-dessus est susceptible de remplir les fonctions d'identification assurées par la signature.

(2) La manifestation du consentement du signataire

La signature atteste la volonté du signataire de donner son approbation finale aux dispositions contenues dans l'acte¹¹. Le texte de l'article 1316-4 établit le lien formel entre l'acte et la signature de l'acte. Ce lien est réalisé par l'**apposition** de la signature. Lorsqu'elle est électronique, le législateur a pris la peine d'explicitier la manière dont cette apposition doit être formalisée. C'est par l'utilisation d'un «*procédé fiable ... garantissant [le lien de la signature électronique] avec l'acte auquel elle s'attache*»¹².

⁸ C. civil, art. 1316.

⁹ C. civil, art. 1316-4.

¹⁰ I. Dauriac, thèse précitée, no. 162 et s.

¹¹ C. civil, art. 1316-4, 1^{er} alinéa.

¹² C. civil, art 1316-4, 2^{ème} alinéa.

Ainsi, les fonctions de la signature électronique se manifestent toujours par rapport à un acte précis, cette signature étant un des éléments constitutifs de cet acte, que celui-ci soit sous seing privé ou authentique.

Pour terminer, le décret apporte une précision supplémentaire quant à la définition de la signature électronique: avant de renvoyer à l'article 1316-4 du Code Civil, l'article 1.1 du décret appréhende cette signature non seulement par rapport à l'**utilisation** du procédé, mais aussi, son **résultat**, c'est-à-dire de la **donnée** qui en résulte.

(B) Les conditions de la fiabilité du procédé de signature

Pour être efficace, la signature électronique doit consister «*... en l'usage d'un procédé fiable...*»¹³. Qu'est-ce qu'un procédé fiable? Au sens technique, fiable se dit d'un «*matériel dans lequel on peut avoir confiance et qui fonctionne bien*»¹⁴. Lorsqu'il s'agit d'un procédé technique, en principe, l'appréciation de la fiabilité relève de l'intime conviction du juge. Les parties ont à apporter la preuve de cette fiabilité. Toutefois, cette fiabilité peut être présumée si certaines conditions sont remplies. Ce sont ces conditions qui font l'objet du décret ici étudié.

(C) La présomption de fiabilité de la signature sécurisée

La loi du 13 mars 2000 a posé le principe d'une présomption de fiabilité des procédés de signature électronique: «*La fiabilité de ce procédé est présumée, jusqu'à preuve du contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État*»¹⁵. L'objectif d'un tel décret doit donc être de fixer les conditions des trois opérations ponctuelles distinctes qu'un procédé de signature doit réaliser pour être présumé fiable:

- la **création** de la signature;
- l'**identification** sûre du signataire;
- et la **garantie** de l'intégrité de l'acte.

¹³ *Idem.*

¹⁴ *Le Petit Robert, Éditions Le Robert, 1993.*

¹⁵ *C. civil, art. 1316-4.*

Alors que la loi laisse ouvert le choix des moyens techniques permettant de réaliser ces trois opérations, le décret étudié dans cet article précise les conditions d'utilisation d'une catégorie particulière de procédés, à savoir ceux mettant en œuvre la signature électronique sécurisée. Avant d'analyser ces conditions et de constater si le décret remplit effectivement les objectifs fixés par la loi¹⁶, il convient de définir la notion de signature électronique sécurisée (1) et de rappeler la signification de la présomption de fiabilité posée par le texte (2).

(1) La signature électronique sécurisée

Le décret poursuit la transposition en droit français de la directive européenne du 13 décembre 1999, en appelant «*signature électronique sécurisée*» ce qui dans la directive est appelé «*signature électronique avancée*». L'article 1.2 du décret la définit comme une signature électronique satisfaisant à trois exigences supplémentaires: «*être propre au signataire*», «*créée par des moyens que le signataire puisse garder sous son contrôle exclusif*» et «*garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable*». Ces exigences viennent affiner les fonctions d'identification et de manifestation du consentement de la signature électronique ordinaire.

(a) Être propre au signataire

«*Propre*» peut être entendu comme «*distinctif*», mais il ne s'agirait pas alors d'une exigence supplémentaire par rapport à la signature électronique. On en déduit donc que «*propre*» doit être entendu ici au sens d'«*exclusif*», c'est à dire qu'il est exclu qu'un signataire puisse, en signant, produire un résultat (donnée) qui puisse être imputé à un autre signataire. De ce fait, le signataire doit disposer de «*données de création de signature*» (par ex., clés privées cryptographiques) qui lui sont personnelles (art. 1.4).

(b) Contrôle exclusif des moyens de signature

Cette exigence apporte également des garanties supplémentaires quant à l'identité du signataire. Elle assure que celui-ci conserve la maîtrise des moyens de signature, soit pour les utiliser lui-même, soit pour

¹⁶ Voir infra.

éventuellement les faire utiliser par d'autres sous sa responsabilité. Cette exigence se justifie si l'on considère que les données de création de signature sont un **secret transférable**.¹⁷

(c) Détection de modifications ultérieures de l'acte

La signature électronique ordinaire consiste « *en l'usage d'un procédé qui garantit son lien avec l'acte auquel elle s'attache* »¹⁸. Dans le cas de la signature électronique sécurisée, ce lien remplit une fonctionnalité supplémentaire: toute modification de l'acte survenant après la signature de l'acte doit pouvoir être détectée, et ce, par le procédé de signature électronique sécurisée. Nous aurons l'occasion de voir plus tard que cette exigence est très problématique.

(2) Le principe de la présomption de fiabilité de la signature sécurisée

Une présomption est définie comme « *une opération de l'esprit par laquelle on admet l'existence d'un fait qui n'est pas directement démontré mais qui est rendu vraisemblable par la preuve supposée ou rapportée d'un autre fait.* »¹⁹ Le principe de présomption de fiabilité des procédés de signature a pour objet d'éviter au juge d'avoir à apprécier les caractéristiques de systèmes techniques complexes. Ceux-ci, s'il est démontré qu'ils correspondent bien aux conditions fixées par le décret, seront présumés fiables.

Cette présomption de fiabilité est simple et établit ainsi un renversement de la charge de la preuve, qui incombe alors à celui qui conteste la fiabilité du procédé de signature utilisé. En principe, contrairement à une présomption irréfragable, la présomption simple permet de remettre en cause la fiabilité du procédé. Toutefois, on peut d'ores et déjà s'interroger sur la capacité des parties à apporter une telle preuve contraire.²⁰

II - Les conditions à remplir pour la présomption de fiabilité

¹⁷ Voir sur ce point *D. Guinier, Une signature numérique insatisfaisante est-elle encore une signature?*, *Gaz. Pal.* 15-19 avril 2000, pp. 14-18.

¹⁸ *C. civil*, art. 1316-4, 2^{ème} alinéa.

¹⁹ Définition empruntée à Domat et reprise par toute la doctrine.

²⁰ Voir sur ce point *D. Guinier, article précité*.

Le décret du 30 mars 2001 détermine ces conditions, qui sont au nombre de quatre: le procédé de signature doit mettre «*en œuvre une signature électronique sécurisée*», celle-ci doit être «*établie grâce à un dispositif sécurisé de création de signature électronique*». Enfin, cette signature doit être vérifiée et cette vérification doit reposer «*sur l'utilisation d'un certificat électronique qualifié*».²¹

Bien que le décret n'utilise pas directement cette terminologie, la signature électronique sécurisée est celle fondée sur les technologies de la cryptographie à clé publique.²² L'utilisation de «*certificats*» pour la vérification n'est en effet compréhensible que dans le contexte de cette technologie.

Pour pouvoir analyser la façon dont le décret transcrit les exigences de la directive relative à ces procédés, nous avons choisi de suivre la chronologie des opérations du processus de signature cryptographique: tout d'abord, la certification, traitée au chapitre III du décret (A); ensuite, la création de signature, traitée au chapitre I du décret (B); finalement, la vérification de signature, traitée au chapitre II du décret (C).

Cette division permet de mettre en relief le fait que, d'une part, chacune de ces étapes fait appel à des procédés techniques et des services différents et d'autre part, que les règles et régimes auxquels sont soumis ceux-ci ne présentent pas le même caractère obligatoire et les mêmes modalités d'accès au marché.

(A) La prestation de services de certification électronique

Le chapitre III du décret transcrit les annexes I («*exigences concernant les certificats qualifiés*») et II («*exigences concernant les prestataires de services de certification délivrant des certificats qualifiés*») de la directive européenne, et organise la fourniture des services de certification et l'agrément par des organismes qualifiés de la conformité de ces services aux exigences du décret. Dans ce chapitre, on trouve à la fois les conditions relatives à l'exécution de la prestation de certification de clés publiques (1) et les conditions auxquelles sont soumises les prestataires de

²¹ Art. 2.

²² Pour des exposés vulgarisés de ces technologies, voir J. Stern, *La Science du secret*, Odile Jacob, 1999 ; G. Dubertret, *Initiation à la cryptographie*, Vuibert, 2000.

services de certification en vue de leur reconnaissance comme prestataire qualifié (2).

(1) Les conditions relatives à la prestation de certification

Avant de détailler les conditions imposées par le décret aux prestataires de services de certification, il convient pour comprendre le rôle de ces services de rappeler brièvement le processus de la signature cryptographique à clé publique.

Création de signature et certification: Chaque utilisateur dispose d'une paire de clés, une publique, accessible à tous, et une privée, que l'utilisateur conserve secrète. Pour échanger un message signé, le signataire utilise sa clé privée et le destinataire utilise la clé publique associée pour vérifier l'origine et l'intégrité du message. Le service de certification apporte la garantie que la clé publique fournie est bien la bonne, en inscrivant la clé publique d'un utilisateur dans un certificat émis à son nom. Ce certificat est lui-même signé par le prestataire avec sa clé privée.

Vérification de signature: le destinataire d'un message signé peut vérifier cette signature en quatre étapes: premièrement, il doit se procurer la clé publique du prestataire de service de certification; deuxièmement, se procurer le certificat du signataire; troisièmement, il vérifie la signature du prestataire sur le certificat, à l'aide de la clé publique du prestataire; quatrièmement, si cette vérification est positive, il utilise la clé publique contenue dans le certificat pour vérifier la signature sur le message.

Les certificats qualifiés: Le décret énonce les éléments obligatoires d'un certificat qualifié (art. 6.I) et les exigences relatives à la prestation de services de certification (art. 6.II). Dans le premier cas, ces éléments concernent à la fois le prestataire de certification et le signataire pour lequel le certificat a été émis. Le premier doit s'identifier (art. 6.I.b), signer le certificat avec une signature électronique sécurisée (art. 6.I.h), indiquer les conditions d'utilisation du certificat, c'est-à-dire sa période de validité (art. 6.I.f) et le montant maximum des transactions pour lesquelles il peut être utilisé (art. 6.I.i). Le second doit être identifié, par son nom ou par un pseudonyme (art. 6.I.c), et sa qualité le cas échéant (art. 6.I.d). Le certificat doit également contenir les données de vérification de signature électronique le concernant (art. 6.I.e). Enfin, le certificat doit comporter

un numéro de série (art. 6.I.g) et porter mention qu'il a été délivré à titre de certificat qualifié (art. 6.I.a).

La prestation de certification: Pour pouvoir être considéré comme qualifié, le certificat doit de plus être émis par un prestataire de services de certification conformes aux exigences énumérées à l'article 6.II. La plupart de ces exigences se rapportent au cycle de vie du certificat (délivrance, utilisation, révocation), les autres relevant d'obligations plus générales et transversales. Parmi ces nombreuses exigences, on attirera l'attention sur le fait que, lors de la délivrance, le prestataire est tenu de vérifier l'exactitude des informations contenues dans le certificat, y compris l'identité (art. 6.II.m, 6.II.n) et la validité de la clé publique (art. 6.II.j); que le prestataire est tenu d'un devoir d'information par écrit à l'égard de son client (6.II.o).

Le prestataire doit fournir un service d'annuaire de certificats (art. 6.II.b); conserver les certificats de façon sécuritaire, pour en prévenir la falsification et permettre leur utilisation comme preuve en justice (art. 6.II.l, 6.II.h et 6.II.k). Il doit organiser un service de révocation de certificat sûr et rapide (art. 6.II.c). Enfin, il doit employer du personnel compétent (art. 6.II.c), appliquer des procédures et utiliser des systèmes de sécurité appropriés (art. 6.II.f et 6.II.g).

(2) les conditions de qualification et le contrôle des prestataires de certification

Finalité de la qualification: Comme la directive l'exige (art. 3.1), aucune autorisation préalable n'est nécessaire pour exercer des activités de prestataire de services de certification. Toutefois, dans le but d'améliorer le niveau du service de certification, le décret met en place, à la suggestion de la directive (art. 3.2), un régime de « qualification » des prestataires (art. 7). Cette qualification vaut présomption de conformité aux exigences énumérées à l'article 6 et présentées ci-dessus. Pour qu'un certificat soit considéré comme qualifié, il doit répondre aux exigences de l'article 6.1 du décret et être émis par un prestataire lui-même qualifié²³. Cette double qualification (des prestataires et des certificats) est donc une condition préalable indispensable à la présomption de fiabilité du procédé de signature électronique sécurisée.

²³ Directive européenne, art. 2.10; Décret du 30 mars 2001, art.6.

Modalités de la qualification des prestataires: Cette qualification suit un mode d'organisation pyramidale, sur trois niveaux: une instance est désignée par le ministre de l'industrie pour accréditer les organismes responsables de l'évaluation et de la qualification des prestataires de services de certification (art. 7). Tant la désignation de l'instance d'accréditation des organismes que les procédures d'évaluation et de qualification seront déterminées par des arrêtés du Premier Ministre et du ministre chargé de l'industrie.

Contrôle des prestataires: La directive suggère (art. 3.3) que chaque État membre assure la mise en place d'un mécanisme de contrôle des prestataires de services de certification établis sur son territoire. Ce contrôle, tel qu'organisé par le décret (art. 9.II) vise tout autant les prestataires qualifiés que ceux non-qualifiés. Il porte sur le respect des exigences définies à l'article 6, et peut être effectué d'office ou à l'occasion de toute réclamation mettant en cause l'activité d'un prestataire, et peut faire l'objet d'une procédure contradictoire. Il est effectué par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information (SCSSI).

Si le prestataire en question est qualifié, et s'il n'a pas satisfait aux exigences de l'article 6, les SCSSI en informent l'organisme de qualification. Lorsque le prestataire n'est pas qualifié, les exigences de l'article 6 ne lui sont pas opposables, mais la publicité par les SCSSI du résultat du contrôle sont une incitation à les respecter.

Pour terminer, il est important d'observer que si le décret remplit correctement l'exigence formelle de libre accès au marché de la prestation de services de certification, la procédure de qualification permet d'instaurer une hiérarchie des prestataires: ceux qui auront été qualifiés et seront de ce fait présumés conformes aux exigences de l'article 6.II, et ceux qui ne sont pas qualifiés et auront à faire la preuve de cette conformité lorsque leur responsabilité est engagée.

(B) La création de signature électronique

La signature électronique est réalisée par l'utilisation d'un dispositif sécurisé mettant en œuvre des données de création de signature électronique. Pour que ce dispositif puisse être qualifié de sécurisé, il doit répondre aux exigences de l'article 3.I du décret, et être certifié conforme

à ces exigences dans les conditions posées à l'article 3.II. Nous examinons ces exigences (1) et la procédure par laquelle un dispositif est certifié conforme à ces exigences (2).

(1) Les exigences

Elles sont au nombre de quatre. Les trois premières visent les moyens techniques de protection des données de création de signature: un dispositif sécurisé de signature électronique doit en assurer l'**unicité** (art. 3.I.1.a), la protection contre la **falsification** et la **dédution** (art. 3.I.1.b), et en permettre une protection efficace par le signataire contre l'**utilisation par les tiers** (art. 3.I.1.c). La dernière exigence vise à garantir que le dispositif ne fasse pas obstacle à ce que le signataire ait une connaissance exacte du **contenu de l'acte** avant de signer, et que le dispositif de signature n'entraîne aucune **altération de l'acte signé** (art. 3.I.2).

Caractère absolu des exigences: On notera tout d'abord que la formulation des articles 3.I.1.a et 3.I.1.b est plus rigide que celle de la directive. Alors que celle-ci relativisait tant la notion d'unicité des données de création de signature (« *les données utilisées pour la création de signature ne puissent, **pratiquement**, se rencontrer qu'une seule fois...* »)²⁴, que leur déduction (« *garantir ... que l'on puisse avoir l'**assurance suffisante** que les données ne puissent être trouvées par déduction...* »)²⁵, le décret supprime ce caractère relatif. On peut regretter ce resserrement des exigences. En effet, même si le risque est infime, aucun mécanisme de création de signature ne serait en mesure de s'y conformer, puisque ces exigences font référence à des processus mathématiques **probabilistes**, et non **déterministes**.

Responsabilité des signataires: On notera ensuite qu'il importe de bien comprendre la portée de l'article 3.I.1.c. Un industriel qui obtient la certification de conformité aux exigences pour le dispositif de création de signature électronique qu'il a conçu, n'est plus responsable de l'utilisation de ce dispositif par des tiers autres que le signataire. C'est ce dernier qui devient alors responsable de la protection de ses données de création de signature. Cette responsabilité devrait pouvoir être appréciée non seulement en tenant compte de la présomption de fiabilité qui résulte de

²⁴ Directive européenne, annexe III, art. 1.a.

²⁵ Directive européenne, annexe III, art. 1.b.

la conformité du procédé aux exigences, mais aussi de la **capacité** du signataire à remplir son obligation et apporter la preuve contraire.

Limites du «What You See Is What You Sign»: En dernier lieu, il convient de relever les nombreuses critiques et commentaires dirigés contre ce concept (ce que vous voyez est ce que vous signez), objet de l'article 3.I.2. De nombreux spécialistes de la cryptologie — dont l'un des auteurs de cet article — considèrent qu'il est, à toutes fins pratiques, impossible d'assurer qu'une telle exigence est toujours remplie²⁶, lorsque le dispositif sécurisé de création de signature est connecté à un système informatique **multi-fonctions**. En effet, celui-ci rend nécessairement le dispositif de signature vulnérable à un piratage visant la **modification du contenu de l'acte** au cours du processus de signature.

(2) La procédure de certification de conformité des dispositifs

Alors que la qualification n'est pas exigée des prestataires de services de certification pour démontrer leur conformité aux exigences du décret, la **certification de conformité est obligatoire** pour qu'un dispositif de création de signature électronique puisse être **considéré comme sécurisé** (art. 3). Ces dispositifs peuvent être certifiés par deux types d'organismes: un organisme désigné à cet effet par un État membre de la Communauté européenne (art. 3.II.2), ou les SCSSI du Premier ministre (art. 3.II.1). Dans ce dernier cas, les mécanismes de certification suivent également un mode d'**organisation pyramidale**, sur deux niveaux: d'une part, un comité directeur de la certification, institué auprès du Premier ministre, assure le contrôle de la mise œuvre des procédures d'évaluation et de certification des dispositifs (art. 4); d'autre part, l'évaluation et la certification sont assurées par des organismes agréés par les SCSSI. Ici aussi, les règles relatives à l'évaluation et la certification sont renvoyées par le décret à des **arrêtés du Premier ministre**. Toutefois, le décret précise d'ores et déjà que la délivrance des certificats de conformité doit être rendue publique (art. 3.II.1).

(C) La vérification de la signature électronique

Finalité de la vérification: Une fois le certificat **établi** et la signature **créée**, celle-ci doit bien entendu être **vérifiée**. Cette vérification est effectuée à partir des données de vérification de signature électronique

²⁶ Par exemple, D. Guinier, *article précité*; Bruce Schneier, *Secret and lies: Digital security in a networked world*. Willey and Sons, 2000.

(c'est-à-dire, la **clé publique**) qui se retrouvent dans un certificat (qualifié ou non). La **validité** d'une signature cryptographique est alors déduite de cette vérification, opération qui fournit trois réponses possibles: soit que la signature est valide, soit qu'elle est invalide, soit que le processus de vérification ne dispose pas des données suffisantes pour fournir une réponse²⁷.

Organisation de la vérification: La **seule exigence** requise par le décret pour qu'un procédé de signature électronique bénéficie de la présomption de fiabilité est que la vérification des signatures repose sur l'**utilisation d'un certificat électronique qualifié** (art. 2), sans toutefois préciser quelles données du certificat sont nécessaires à la vérification. D'autre part, le décret définit la notion de «**dispositifs de vérification de signature électronique**» (art. 1.7) et organise de façon détaillée leurs conditions de certification (art. 5).

On pourrait alors s'étonner que, contrairement au cas des opérations de création de signature, le décret n'exige, ni la certification des dispositifs de vérification, ni même leur **utilisation**, que ceux-ci soient certifiés ou non. L'origine de cette différence se trouve dans la directive, qui pose aux dispositifs de vérification de signature, non pas des exigences, (comme c'est le cas pour les dispositifs de création de signature) mais uniquement des **recommandations** (annexe IV). Pour assurer la sécurité minimale des dispositifs de vérification, la directive engage uniquement la Commission et les États membres à «**promouvoir la mise au point et l'utilisation**» de tels dispositifs, et ce, «**dans l'intérêt du consommateur**» (art. 3.6).

Bien que la certification des dispositifs de vérification soit facultative, nous examinons d'une part les conditions posées par le décret pour cette certification (1), et d'autre part, le problème de la pérennité de ces signatures, dans le décret et au delà (2).

(1) Les conditions de certification des dispositifs de vérification

Cette certification est obtenue, après évaluation, selon des règles précisées par arrêté du Premier ministre (art.5, premier alinéa). Les dispositifs de vérification doivent remplir un certain nombre de fonctions: vérifier l'**exactitude** de la signature (art. 5.b), les **conditions d'utilisation** et la

²⁷ Voir à ce sujet D. Pinkas, *Using Signature Policies to verify E-Signatures*, présentation faite à la conférence ISSE 2000, Barcelone, 4 octobre 2000, qui résume l'approche du projet EESSI, consortium européen de standardisation de la signature électronique.

durée de validité du certificat électronique (art. 5.d); porter obligatoirement à la connaissance du vérificateur l'**identité du signataire** (art. 5.e), éventuellement son **pseudonyme** (art. 5.f), ainsi que le résultat des vérifications mentionnées ci-dessus (art. 5.b, art. 5.d in fine); permettre au vérificateur de déterminer, si nécessaire, le **contenu** des données signées (art. 5.c); enfin, le dispositif doit pouvoir détecter toute **modification** ayant une incidence sur la vérification (art. 5.g). Cette dernière condition impose que la vérification d'un document signé ayant subi une modification ultérieure à la signature résulte en l'invalidité de la signature. Qu'en est-il lorsque ces modifications sont rendues nécessaires pour assurer la **lisibilité** pérenne du document?

(2) Le problème de la pérennité des signatures électroniques sécurisées

Il convient d'observer que le décret, tout comme la directive, ne fait aucune distinction entre **deux types** de vérification bien distincts: une **première** vérification, qui est celle effectuée par le **destinataire** du message au moment où il reçoit le document signé; et une **seconde**, qui serait effectuée, longtemps après, par exemple, par un **juge** ou un **expert**²⁸. Le vérificateur, selon qu'il est le destinataire original du message, ou le juge/expert, sera confronté à des conditions techniques très différentes. Dans le premier cas, la **période écoulée** entre la création de la signature et sa vérification sera probablement **courte**, alors que dans le second cas, l'écart entre création et vérification peut être **très long**, en fonction des délais de prescription. Ainsi, cette dernière vérification s'effectuera sur un document signé qui aura fait l'objet d'un processus d'**archivage électronique**.

Dans le but d'assurer leur lisibilité pérenne, ce processus implique des **migrations périodiques** des documents archivés, migrations qui modifient nécessairement les documents signés. Selon l'exigence de l'article 5.g, du décret, ces modifications entraîneront donc l'**échec** du processus de vérification des signatures. Les contraintes techniques visant à assurer la **vérification pérenne** des signatures sont donc incompatibles avec celles visant à assurer la **lisibilité pérenne** des documents. Des solutions de « re-signature » ou de « sur-signature » sont généralement proposées pour pallier au problème de la vérification pérenne des signatures électroniques sécurisées²⁹. Malheureusement, elles ne permettent pas non plus de réaliser **simultanément** les objectifs de

²⁸ Voir Pinkas, *article précité*.

²⁹ Voir à ce sujet *Vers l'authenticité électronique, 10ièmes rencontres notariat-université, Petites affiches, 2 avril 2001, en particulier, P.-A. Fouque, Les technologies de l'écrit électronique, pp. 8-14; P. Leclercq, Rapport de synthèse, pp. 35-39.*

lisibilité des documents et de vérification (c'est-à-dire d'intelligibilité) des signatures.

Ainsi, il faut se demander si l'une des finalités de la signature électronique sécurisée — celle d'assurer l'intégrité pérenne du document signé grâce au processus de vérification — peut être véritablement assurée.

Conclusion

Sur la base de ces observations, il convient de formuler un certain nombre d'interrogations: le décret remplit-il bel et bien les **objectifs** qui lui avaient été assignés par la loi? (1); quel sont les **limites** de la preuve fournie par la signature électronique sécurisée? (2); quelles sont les **conséquences** juridiques liées aux problèmes de vérification des signatures électroniques sécurisées? (3).

(1) Les objectifs assignés au décret par la loi du 13 mars 2000

Si les deux premiers objectifs (création de la signature, identification sûre du signataire) semblent être correctement remplis, on peut se demander si le décret a vraiment pris en compte la question délicate de la garantie de l'intégrité à long terme de l'acte signé. Les problèmes que nous avons soulevés à propos de la vérification pérenne des signatures électroniques sécurisées montrent qu'il est nécessaire d'élaborer de façon beaucoup plus précise les exigences relatives à la conservation des actes. Ces exigences devraient prendre en compte le **double objectif** de l'intelligibilité pérenne des actes et des signatures qui y sont apposées.

(2) Les limites de la preuve fournie par la vérification

Même dans le cas où il est possible d'effectuer l'opération de vérification d'une signature électronique sécurisée, il est intéressant de se demander quelles sont les **limites** de la preuve apportée par cette vérification. Le processus de vérification est en effet une opération mathématique, réalisée informatiquement, qui produit trois résultats possibles: «**signature valide**», signature «**invalidé**», et «**pas de réponse**». Ces trois résultats résument des opérations techniques et mathématiques très complexes, et sont en quelque sorte un acte de foi en ces opérations.³⁰ Si la

³⁰ Pour un débat similaire chez les mathématiciens, voir R. A. De Millo, R. J. Lipton et A. J. Perlis, *Social processes and proofs of theorems and programs*, *Communications of the ACM*, mai 1979, vol. 22, no. 5, 271-280.

vérification est positive, il est fortement probable que la signature soit effectivement valide. Par contre, si la vérification est négative, les causes de cette invalidité peuvent être diverses: la clé de vérification ne correspond pas à la clé de signature; le document signé, ou le certificat ont été modifiés; le processus de vérification n'a pas fonctionné correctement, par exemple, par simple incompatibilités de systèmes, de logiciels, etc. Il sera difficile de tirer les conséquences de cette vérification négative sans rechercher les causes plus précises de l'invalidité de la signature.

(3) Les conséquences juridiques liées au problème de la pérennité des signatures électroniques sécurisées

Les problèmes que nous avons soulevés invitent à revoir les exigences de la signature électronique sécurisée, qui sont peut être trop larges. Ne faut-il pas dissocier les fonctions d'identification et la manifestation de la volonté du consentement propre à toute signature, de celle de garantie de l'intégrité, spécifique à la signature électronique sécurisée du décret? Rien n'exige que cette garantie repose principalement sur le mécanisme de signature lui-même, celle-ci pouvant tout autant être fondée sur des mécanismes techniques, que procéduraux ou institutionnels. Le principe de non-discrimination énoncé à l'article 5.2 de la directive ne dit pas autre chose, et la réflexion en cours sur les actes authentiques électroniques en a tiré toutes les conséquences.

La sécurité juridique passe par une certaine stabilité du droit et, par conséquent, par l'aptitude des règles générales à appréhender des objets nouveaux tout en restant indépendantes de l'évolution de la technique. Il faut aussi rester vigilant et ne pas faire du recours aux techniques une fin en soi, leur obsolescence inévitable imposant une certaine prudence pour ne pas enfermer le cadre juridique. Ainsi, on pourrait regretter que ce décret soit interprété comme fondant uniquement la sécurité juridique sur la technique: compte tenu de l'état embryonnaire des connaissances relatives à la conception, au déploiement et à l'utilisation des technologies de signature électronique, cette interprétation pourrait entretenir une illusion de sécurité.