Le lisible et l'illisible

The Legible and the Illegible

Sous la direction de
Ysolde Gendreau
Editor

Les Éditions Thémis

CRDP

Université de Montréal

Lisibilité et illisibilité dans la société de l'information – Réflexion à propos de l'anonymisation et de l'archivage

Isabelle de Lamberterie*

* Directrice de recherche, CNRS-CECOJI, France.

Parmi les défis lancés à la Société de l'information, il y a entre autres la recherche d'équilibre entre des droits et des principes qui apparemment pourraient être perçus comme contradictoires. Comment protéger la vie privée tout en garantissant un droit à l'information surtout quand il s'agit de données publiques? Comment garantir l'intégrité de certains documents numériques par des procédés techniques sans hypothéquer la pérennité sur le long terme de ces documents numériques ? Telles sont quelques-unes des questions fondamentales qui montrent la complexité à laquelle doivent faire face ceux qui ont en charge la régulation de cette société.

Prise indépendamment, chaque branche du droit concernée a sa logique et sa cohérence qu'il s'agisse d'informatique et de libertés, des droits du citoyen à disposer des données essentielles, de la sécurité technique indispensable ou encore de la nécessité d'organiser la conservation ou l'archivage des documents numériques.

Néanmoins, il est indispensable que ces logiques se rencontrent ou du moins coexistent quand il s'agit du dénominateur commun qu'est l'information. Et pourtant qu'il s'agisse du droit à l'information ou du droit sur l'information, les intérêts divergent et même s'opposent. Notre réflexion s'inscrit ici dans un cadre transversal autour des notions de lisibilité et d'illisibilité : lisibilité du droit mais aussi demande de lisibilité ou d'illisibilité générée par le droit.

En effet, l'information doit être plus ou moins lisible, directement ou indirectement, en fonction du contexte dans lequel elle est diffusée, des finalités pour lesquelles elle est traitée ou communiquée, des autres informations dont dispose le destinataire. Cette lisibilité n'est-elle pas alors réservée à ceux qui y sont autorisés?

Rendre illisible une information peut, aussi, être une exigence imposée par le droit au même titre qu'assurer la lisibilité pour l'avenir.

Si, le plus souvent, chacune de ces situations est étudiée dans son contexte avec ses spécificités et ses finalités, ces problématiques révèlent des constantes propres à la société de l'information. Parmi celles-ci, on relèvera ici l'étroite imbrication entre différents « objets » de droit. Pour appréhender le cadre juridique de l'information, il faut prendre en compte, à la fois, le contenu informationnel qui peut être ou non l'objet de droit privatif avec le « contenant » à savoir le « document » au sein duquel se trouve fixée cette information de manière à être rendu accessible. L'exemple des bases de données illustre bien cette dualité.

On soulignera aussi, le besoin d'assurer à la fois le traitement, la circulation et la conservation tant de l'information que des documents contenant l'information. Ces opérations s'inscrivent à la fois dans un contexte culturel, politique, géographique (celui dans lequel nous vivons – à savoir la société civile) et dans un contexte supra national qui dépasse les frontières, les barrières culturelles et géopolitiques traditionnelles. Chacun de ces contextes engendre un besoin spécifique et il s'avère parfois difficile de les concilier. On mesure alors l'intérêt d'une démarche comparative, la richesse d'une certaine distanciation par rapport à la réalité juridique telle qu'elle est mise en œuvre en ce moment en France ou au Québec. La question n'est pas de faire du mimétisme et de vouloir plaquer les expériences des autres. Il faut, bien au contraire, analyser les raisons profondes qui nous conduisent à réagir autrement. Cela permet de faire la part des raisons culturelles, historiques ou juridiques qui peuvent être sources de blocage à la recherche d'un tronc commun indispensable dans une société.

Ce travail de comparaison est pour l'instant, encore, très embryonnaire et mérite d'être approfondi sur les questions essentielles sur lesquelles nous ouvrirons quelques pistes.

Mettre en contexte, définir, qualifier, tel sera le point de départ de cette approche. Il convient donc, de replacer cette analyse au sein de la Société de l'Information.

Nous traiterons, donc, de la lisibilité ou de l'illisibilité au service du droit. « Lisible », « illisible », ces adjectifs renvoient – dans la langue courante – au fait de pouvoir – ou de ne pas pouvoir – lire, déchiffrer une écriture, un texte, une signature. Ce sens courant vaut pour la Société de l'Information et nous connaissons tous, le problème du disque ou de la disquette illisible. C'est ce sens que nous reprendrons quand nous traiterons de la lisibilité souhaitée, espérée des supports informatiques sur lesquels peuvent avoir été conservés et archivés des informations, des documents qui ont pour vocation d'être accessibles aux générations à venir.

Le terme lisible peut aussi être entendu au sens figuré : à savoir ce qui doit pouvoir être compris (lisibilité d'un texte, transparence et accessibilité des informations contenues dans ce texte). Nous reprendrons ce deuxième sens à propos de la protection de la vie privée au regard du traitement de l'information. La lisibilité correspond à l'identification nécessaire ou voulue, l'illisibilité à une anonymisation qui peut être revendiquée.

La lisibilité peut ainsi être perçue comme une menace à la protection de la vie privée (I). Elle reste néanmoins une garantie à préserver dans le cadre de la conservation et de l'archivage à long terme des actes authentiques (II).

I. La lisibilité : menace à la protection de la vie privée

Le titre donné à la directive communautaire de 1995[1] exprime clairement la finalité de ce texte : assurer la protection de la vie privée au regard du traitement de l'information. Comme dans la loi française de 1978[2], le principe est posé que le traitement des informations nominatives ou des données personnelles peut être une atteinte à la vie privée de celui qui est concerné par ces informations.

On rappellera le contexte historique dans lequel se sont inscrits ces textes puis on tentera de cerner quand et jusqu'où la notion d'information nominative *lisible* peut être une menace pour la protection de la vie privée.

A. Le contexte et les données du débat

Avec le développement de l'informatique, le besoin s'est fait sentir dans les années 70 d'organiser la défense des libertés individuelles au regard du traitement de l'information automatisé. Il s'est agi à l'époque d'un véritable débat de société qui a abouti en France au vote de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Il en a été de même dans de nombreux autres pays. Eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel, les États membres du Conseil de l'Europe ont signé une convention le 28 janvier 1981[3]. Près de dix ans après la Convention du Conseil de l'Europe, la Commission des Communautés européennes a

---

1 *Directive 95/46/CE du Parlement européen et du conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.*

2 *Loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. du 7 janv. 1978.

3 *Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.*

jugé nécessaire de relancer le débat avec la directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Ces textes affirment tous le principe de la protection de l'identité humaine au regard du traitement des informations nominatives : l'informatique ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Les données à caractère personnel étant un révélateur des éléments de la vie personnelle intime, le traitement automatisé de ces informations nominatives est exclu, limité ou encadré.

De plus, il est largement admis que le droit à la vie privée est mis en péril non pas uniquement par le contenu des données à caractère personnel mais par le contexte dans lequel se situe le traitement de ces données. Il s'agit de prendre en compte la finalité du fichier et du traitement des données. Enfin, certaines catégories de données sont, de par leur contenu, plus ou moins sensibles et méritent, à ce titre, une protection particulière.

B. Qu'est-ce qu'une information nominative?

L'article 4 de la loi de 1978 précise ce que sont les informations nominatives :

> « Sont réputées nominatives au sens de la présente loi les informations qui permettent sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale ».

La directive européenne utilise l'expression « données à caractère personnel ». Une donnée à caractère personnel est définie dans l'article 2 (a) comme « toute information concernant une personne physique identifiée ou identifiable. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence ».

L'information nominative (ou la donnée personnelle) est celle qui permet l'identification de la personne, cette identification pouvant être directe ou indirecte.

Au-delà du nom sont ainsi englobés dans les informations nominatives tous les renseignements qui concernent une personne physique et permettent de l'identifier[4].

C. Dans quelles conditions peut-on traiter et conserver des données nominatives? Le principe de finalité

Le principe de finalité consiste à garantir que dans le cas où des informations nominatives seraient collectées et que la finalité de cette collecte et du traitement a été déterminée, ces données ne puissent être utilisées pour d'autres finalités. Si l'opportunité d'un changement de finalité se présente, le traitement sera considéré comme un nouveau traitement soumis aux obligations légales.

Enfin, la durée de vie des données est liée à leur finalité et les intéressés peuvent exiger que celles-ci soient détruites si elles ne sont plus nécessaires au traitement prévu initialement. Dans l'ancien article 28 de la loi de 1978 il était dit que « Sauf dispositions législatives contraires, les informations ne doivent pas être conservées sous une forme nominative au-delà de la durée prévue à la demande d'avis ou à la déclaration... ». Depuis la loi du 12 avril 2000, la destruction des données

[4] L'article 54 de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels reprend en ces termes le concept de nominatif.

souffre des exceptions pour certaines finalités (statistiques, scientifiques, historiques). Leur conservation n'est alors autorisée que pour ces finalités[5]. La conservation de ces données n'implique pas que toutes puissent être utilisées pour des traitements automatisés pour des finalités statistiques, scientifiques ou historiques. Certaines plus sensibles que d'autre ne peuvent être traitées sans l'accord exprès des intéressés ou l'autorisation de la Commission Informatique et Libertés dans la mesure où l'intérêt des personnes concernées ou encore des motifs d'intérêt général est démontré.

Il est aussi des situations où les finalités du traitement ne justifient plus de garder des données nominatives. Il sera alors question d'anonymisation.

D. Le passage du nominatif à l'anonymat : qu'est-ce qu'une donnée anonyme?

Quand il faut – à un moment ou un autre dans le processus du traitement – respecter le principe de finalité et le droit à la destruction des données, la conservation des données s'accompagne d'un processus de transformation de celles-ci de données identifiantes à données non identifiantes.

En effet, « anonyme »[6] peut être considéré comme l'antonyme d'« identifié ». Un ouvrage anonyme est sans nom d'auteur, une société anonyme est une société dont les propriétaires restent inconnus du public.

---

5 Nouvel article 28 I de la loi du 6 janvier 1978 (modifié par l'article 5 de la *Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations*).

6 Dans Gérard CORNU, Vocabulaire Juridique, 8e éd., Paris, P.U.F., 2000, p. 58 : « Anonyme » (1) Qui n'a pas de nom patronymique [...] (2) Qui ne porte pas de nom de personne.

Une donnée anonyme est une donnée qui ne peut être rattachée à une personne physique. Le processus d'anonymisation, auquel sont tenus ceux qui souhaiteraient utiliser des données nominatives, consiste, donc, en la destruction (effacement) des identifiants.

Une fois le fichier anonymisé, son traitement ne relève plus des contraintes des lois sur la protection de la vie privée au regard du traitement de l'information et l'on mesure l'importance à accorder aux frontières entre nominatifs et anonymes[7].

E. Où commence l'anonymat? Où s'arrête l'indirectement nominatif?

Pour apporter quelques éléments de réponse à cette question, il convient de cerner la notion d'identifiant direct ou indirect. Une donnée qui apparemment peut être considérée comme anonyme peut, en fait, être indirectement nominative.

Qu'est-ce qu'un identifiant?

[7] La question de l'anonymisation se pose aussi – en particulier en France – dans un autre type de circonstances avec la mise à disposition des décisions de jurisprudence à un large public. Certains pensent qu'il y a un risque d'atteinte à la vie privée des parties si on laisse le nom de celles-ci dans les bases de données de jurisprudence. D'autres défendent le point de vue inverse en rappelant que les jugements sont des données publiques et que l'anonymisation va à l'encontre de la publicité des jugements. Ce débat qui dépasse largement le cadre de cette contribution. On renverra au rapport de synthèse du professeur Vincent Gautrais (lors de la 4e conférence internationale « Internet pour le droit », 2-4 octobre 2002, ainsi qu'à la recommandation de la Commission nationale informatique et liberté du 29 novembre 2001 portant sur la diffusion de données personnelles dans Internet par les banques de données de jurisprudence (http://www.cnil.fr).

Est un identifiant une donnée ou un ensemble de données qui se caractérisent par le fait qu'il renvoie à une personne de façon univoque (*unicité*). Le nom, même complété par d'autres informations (prénom, adresse, etc.) offre-t-il toujours cette certitude? Que dire des patronymes très fréquents – comme les Martin, Dupont... Même avec un prénom, il est rarement possible d'identifier une personne unique. D'autres informations s'avèrent nécessaires pour que l'on puisse renvoyer à une personne précise et à elle seule.

La qualité d'identifiant dépend aussi de l'aptitude du destinataire à identifier la personne à travers les données la concernant. Autrement dit, un identifiant identifie une personne *pour* quelqu'un.

On mesure à travers cette analyse la relativité d'un identifiant qui n'est pas lisible pour tout le monde. On mesure aussi qu'une donnée qui apparemment peut sembler être anonyme ne l'est pas pour celui qui a le pouvoir d'identifier une personne, à travers cette donnée.

L'identification est ou non possible, non pas tant selon les caractéristiques du fichier ou des données en elles-mêmes, mais plutôt en fonction de l'information dont dispose le destinataire et de sa capacité à la lire.

Ce constat permet de mesurer les limites d'une protection de la vie privée fondée sur une opposition – *in abstracto* – entre anonyme et nominatif. Pour apprécier les risques effectifs d'une possible atteinte ne doit-on pas prendre en compte les éléments du contexte; la volonté du destinataire de l'information à procéder à une identification – que les données soient ou non anonymes; les informations dont celui-ci dispose pour effectuer la recherche d'identification?

Quels pourraient être alors les critères pour caractériser le vraiment *non identifiable*? Faut-il prendre en compte les efforts « déraisonnables » ou « disproportionnés » indispensables pour arriver au résultat escompté – à savoir identifier une personne à partir des données recueillies? Cette solution a été évoquée lors de la préparation de la directive européenne

sans être retenue dans le texte final. Force est de constater le caractère relatif de la notion.

Celle des risques induits par l'identification est, elle aussi, relative. Comment, alors, prévenir ces risques?

Le projet de loi québécois sur la Société de l'Information[8] apporte sur ce point une position intéressante. Il ne se situe plus sur le point de savoir quelle est la catégorie des données (anonymes ou nominatives directement ou indirectement). Il propose de répondre aux besoins de protection en envisageant une restriction de l'utilisation des fonctions de recherche extensive sur les informations nominatives (article 24). Cette piste mérite l'attention qui convient. Il s'agit là d'un exemple où la technique intervient dans le processus de régulation[9] pour assurer la finalité de l'anonymisation : protéger la vie privée.

On retrouvera cette même interaction entre droit et technique dans l'analyse du cadre juridique dans lequel s'inscrit la lisibilité espérée de certains documents archivés.

II. La lisibilité espérée : la conservation des actes authentiques électroniques

Peut-on conserver des informations nominatives? La logique de la protection de la vie privée est-elle compatible avec les fondements de la politique d'archivage?

---

8 Loi concernant le cadre juridique des technologies de l'information, projet de loi n° 161, présenté par D. Cliche, 2000.

9 Voir sur ce point le travail présenté par Eric Labbé sur « la portée normative des technologies Internet et son encadrement juridique (séminaire doctoral 12 mars 2001).

Une réforme récente de la loi française sur les archives apporte un élément de réponse[10] et pose un principe général. Les informations – même nominatives – collectées dans le cadre de traitements automatisés présentant un intérêt scientifique, statistique ou historique, peuvent être conservées au-delà de la durée prévue lors de la collecte. Ce texte organise les modalités du tri et les conditions de la destruction des informations qui ne présentent pas d'intérêt.

Toutefois ce principe du tri en fonction de l'intérêt des informations contenues ne s'applique pas à certains documents qui de par leur nature sont considérés comme remplissant les conditions pour être conservés et archivés, quand bien même, ils contiennent des informations nominatives. Il s'agit des actes authentiques. Pour eux, il n'est plus question ni de tri, ni de destruction. De plus, les modalités de conservation et d'archivage doivent permettre de les rendre accessibles aux générations futures. Leur lisibilité est espérée voire exigée!

A. Le contexte de cette réflexion : une finalité probatoire et patrimoniale[11]

L'article 1317 du Code civil qui définit l'acte authentique est complété par un 2e alinéa qui dit qu'un acte authentique peut être dressé sur un support électronique s'il est établi et conservé dans des conditions fixées par décret en conseil d'État.

---

10 Art. 4-1 de la loi n° 2000-321 du 12 avril 2000.

11 Les réflexions qui suivent sont tirées des travaux du groupe pluridisciplinaire initié par la mission de recherche Droit et Justice, composée de juristes du monde académique, de professionnels du droit (notaires, avocats, huissiers, magistrats, responsables de l'état civil, greffiers, etc., de spécialistes du traitement de l'information et de la conservation (archivistes, informaticiens). Les résultats de ces travaux ont été publiés dans la collection « Perspectives sur la Justice » de la mission de recherche (Isabelle de Lamberterie, directrice), *Les actes authentiques électroniques. Réflexion juridique prospective*, la Documentation française, avril 2002.

Nous n'aborderons ici que les questions soulevées par la conservation[12] de ces actes sur un support électronique, le terme « conservation » couvrant aussi bien les moyens mis en œuvre pour assurer l'intégrité de l'acte à court terme (tenue des registres) que sa pérennité à long terme (archivage).

En effet, les actes authentiques constituent des archives au sens de la loi française de 1979[13].

Cette loi définit les archives comme « l'ensemble des documents quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité ».

La conservation de ces documents est, alors, organisée « dans l'intérêt public tant pour les besoins et la justification du droit des personnes physiques ou morales, publiques ou privées, que pour la documentation historique de la recherche[14] ».

C'est donc pour répondre à une double finalité probatoire et patrimoniale que cette conservation doit être assurée. Bien que cela ne soit pas pour l'instant explicité dans les textes, on peut comprendre que, pour remplir cette finalité, tout doit être mis en oeuvre afin de garantir pour l'avenir, la lisibilité et l'accessibilité du contenu.

---

[12] On trouvera une analyse détaillée des questions relatives à l'établissement d'un acte authentique électronique dans le rapport remis au ministère de la Justice en vue de la préparation du décret sur l'établissement et la conservation des actes authentiques électroniques.

[13] Art. 3 de la Loi n° 79-18 du 3 janvier 1979 sur les archives.

[14] Art. 1 de la loi du 3 janvier 1979.

Il est intéressant de noter que cette exigence est explicite dans le projet de loi québécois n° 161[15]. À l'article 23 il est dit « que tout document auquel une personne a droit doit être intelligible soit directement soit en faisant appel aux technologies de l'information ».

Compte tenu du fait que les archives publiques sont imprescriptibles[16], comment assurer la lisibilité pour les générations à venir de ces archives établies sur des supports électroniques?

B. Les modalités de la conservation sur un support électronique

La question de la conservation peut apparaître comme un problème « classique » qu'il faut régler, principalement, en tenant compte de sa finalité. Ne rencontre-t-on pas des problèmes techniques pour la conservation des registres papiers?

Le souci de la pérennité de l'acte authentique et de son intangibilité (ou intégrité) se trouvent déjà dans les textes actuels.

Pourtant, la logique de l'usage de l'électronique invite, aussi, à penser autrement la conservation sans transposer, obligatoirement, à ce nouveau support les catégories du papier.

La technique elle-même rend nécessaire une nouvelle approche. La question n'est pas uniquement celle du support et de sa pérennisation (papier, électronique, etc.). Il faut, par exemple, tenir compte des procédés utilisés pour apporter la garantie que le document n'a pas été modifié.

Ce bouleversement technologique peut aussi inviter à repenser la structure institutionnelle de la politique de l'archivage. Enfin, une politique de conservation impose une anticipation du processus et une prise

---

15 www.autoroute.gouv.qc.ca/projet-loi.

16 Art. 3 de la loi n° 79-18 du 3 janvier 1979 sur les archives.

en compte dès la phase d'établissement de l'acte des contraintes inhérentes à la conservation à long terme.

C. Comment faut-il conserver le document? Comment assurer à la fois son intégrité et sa lisibilité?

Point n'est besoin d'être informaticien pour prendre conscience que la conservation des documents électroniques ne peut être envisagée sans des migrations régulières sur de nouveaux supports avec de nouveaux logiciels. Dans la mesure où il semble irréaliste de conserver à la fois les documents et les outils qui ont permis leur création et leur exploitation, il faut organiser, chaque fois que cela sera nécessaire, un transfert des documents devant être conservés afin de ne pas hypothéquer leur lisibilité pour les générations futures.

Deux questions se posent alors pour apprécier ce que signifie la lisibilité d'un document conservé :

- D'une part, on peut se demander si ce qui importe c'est uniquement le *contenu* des informations du document ou s'il faut aussi attacher une importance à la présentation spatiale du document numérique.

- D'autre part – et particulièrement pour certains types de documents comme les actes authentiques – la lisibilité exigée ne signifie-t-elle pas que le document conservé doit se présenter avec tous les éléments qui le composent (toutes les données) lors de son établissement?

D. Contenu et présentation d'un document numérisé

Le document doit-il se présenter tel qu'il était lors de son établissement? Cette question est, bien entendu, très importante quand il s'agit de document dont l'établissement a été soumis à un certain formalisme.

La question est cruciale quand certains éléments essentiels du document – comme la signature – sont difficilement appréhendables (comment représenter un code?).

Le fait même de poser la question peut-il être considéré comme une confusion entre le document et sa représentation papier?

Garantir la « lisibilité » externe d'une signature électronique comme aménager l'organisation spatiale d'un acte sont non seulement des moyens de rassurer mais aussi des moyens de faciliter la lecture de l'acte en aidant le lecteur à trouver ses repères.

La « lisibilité » de la signature peut être nécessaire pour distinguer le simple acte préparatoire numérisé et non encore signé et l'acte authentifié par la signature de l'officier public. On peut alors envisager – comme l'a suggéré le Conseil supérieur du notariat en France, d'assortir l'acte signé de marques distinctives pour faciliter la reconnaissance des actes authentiques. Ce pourrait être, suivant les cas, une image numérisée ou scannée de la signature manuscrite ou un signe correspondant au sceau de l'État.

La formalisation spatiale de l'acte authentique électronique contribue, ainsi, à répondre à une demande de sécurité juridique légitime.

E. Le cas particulier de la signature électronique cryptographique

Lors de l'établissement d'un acte électronique le souci de ceux en charge de cet établissement est de réunir les éléments essentiels de cet acte qui lui confèrent son statut (force probatoire entre autres différente suivant qu'il s'agit d'un acte authentique ou sous seing privé). Parmi ces éléments essentiels, la signature de l'acte joue un rôle particulier. Cette signature quand elle est électronique remplit les mêmes fonctions que toute signature à savoir identifier le signataire et authentifier que celui-ci adhère au contenu de l'acte.

Les besoins de sécuriser la circulation des actes ont rendu nécessaire la prise en compte d'une nouvelle fonction de la signature : assurer l'intégrité de l'acte. On parle alors – en France – de signature électronique *sécurisée*[17]. Dans la directive européenne[18], il est question de signature *avancée*.

Si ces textes reconnaissent la possibilité pour une signature de remplir à la fois les fonctions classiques et la garantie que l'acte signé n'a pas été modifié, la directive européenne comme la loi française font la distinction entre la signature électronique et la signature sécurisée ou avancée. Ces textes tout en reconnaissant la valeur juridique d'une signature électronique quand celle-ci n'est pas sécurisée ou avancée[19], recommandent l'utilisation des procédés de signature cryptographique à clés publiques en posant le principe d'une présomption de fiabilité du procédé[20].

Le problème de la conservation de ce type de signature se pose aujourd'hui. Du fait des techniques utilisées, la migration d'un document signé de cette manière entraîne irrévocablement la destruction de la signature. Soit le document est conservé avec tous les éléments qui le composent et il est alors illisible. Soit sa lisibilité est sauvegardée mais c'est au prix de la disparition de la signature initiale si celle-ci assure à la fois les différentes fonctions d'une signature plus la garantie de l'intégrité du document.

Face à ce problème, aujourd'hui encore insoluble, il apparaît essentiel de prendre en compte dès l'établissement de l'acte les difficultés liées à sa conservation.

---

17 *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique.*

18 *Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.*

19 Art. 5 de la directive sur la signature électronique.

20 Art. 2 du décret n° 2001-272.

C'est pourquoi, il faudrait dissocier pour les documents qui doivent être conservés à long terme, les fonctions de signature et les fonctions visant à garantir l'intégrité. On aurait ainsi, d'une part la signature électronique faisant partie des données initiales du document et pouvant être conservée comme le document électronique et d'autre part la signature électronique sécurisée qui garantirait l'intégrité du document. Celle-ci pourrait disparaître lors de la migration sans incidence sur le contenu initial du document. Elle pourrait aussi être remplacée par une nouvelle signature sécurisée garantissant que la migration n'a aucunement modifié les données initiales.

Ces réflexions sur la sauvegarde de la lisibilité des supports et procédés informatiques nous ont projetés dans l'avenir. La conservation des documents électroniques concerne-t-elle uniquement les archives traditionnelles numérisées ou établies dès l'origine sur un support électronique? La société de l'information n'est-elle pas en train de générer de nouveaux types de documents qui eux aussi représentent une valeur historique et culturelle? Comment appréhender la conservation de ce qui circule sur Internet? Faut-il les conserver et organiser d'ors et déjà leur lisibilité pour les générations futures? Ce sujet est à l'ordre du jour au Québec comme en France :

- En France ceux qui ont pris connaissance de l'avant-projet de loi sur la société de l'information, ont pu constater que cette question était abordée[21].

- Au Québec l'article 68 du projet de loi n° 161 prévoit que le gouvernement peut, par voie réglementaire, déterminer « des critères qui permettent de reconnaître qu'un document – sur son support d'origine – présente une valeur archivistique, historique ou patrimoniale ».

[21] Voir le chapitre IV sur le dépôt légal des services de communication en ligne.

Ces questions dépassent largement un aménagement législatif technique. Raisonner ainsi serait méconnaître ce qu'est aujourd'hui la société de l'information. Nous en sommes tous les acteurs et souhaitons être à même de contribuer à la construction de son avenir en débattant au grand jour, de façon *lisible* et *compréhensible* pour tous, des productions et des valeurs qu'elle compte promouvoir.

9 782894 001561