Date : 09/08/2008 (2nd Version)

L'édition électronique authentifiée de la législation en Europe

Authentication of digital legal information in Europe

Pascal PETITCOLLOT
Secrétariat général du Gouvernement français,
rédacteur en chef de Legifrance
(www.legifrance.gouv.fr)
Paris, France

General Secretariat of the French Government, Head Editor of Legifrance (www.legifrance.gouv.fr)
Paris, France

Meeting: **157. Law Libraries, Library and Research Services for Parliaments, Government Libraries, Government Information and Other Publications**
Simultaneous Interpretation: English-French and French-English only

WORLD LIBRARY AND INFORMATION CONGRESS: 74TH IFLA GENERAL CONFERENCE AND COUNCIL
10-14 August 2008, Québec, Canada
http://www.ifla.org/IV/ifla74/index.htm

Introduction

En Europe, comme en Amérique, on se préoccupe de l'accessibilité permanente et de la conservation à long terme des données juridiques numérisées, car c'est la garantie d'une juste application du droit dans l'avenir, lorsque les supports papiers officiels auront achevé leur déclin irréversible.
Cependant, cette garantie ne peut être effective qu'à condition que l'exhaustivité et l'authenticité de ces données soient assurées, condition indispensable à leur fiabilité et donc à la sécurité juridique.

L'authentification des données juridiques numérisées fait donc partie des sujets de concertation prioritaires dans ce domaine, entre les vingt-sept Etats-membres et les institutions de l'Union Européenne.

En l'espèce, la sécurité juridique et la sécurité technique sont étroitement liées.

Avant de faire le point de la situation, il convient de rendre compte de l'état de la numérisation des données juridiques et de leur conservation à long terme en Europe.

A) La conservation à long terme des données juridiques numériques en Europe *(Long-term preservation of digital legal information in Europe)* :

1) la législation et la jurisprudence *(Legislation and case law)*

Les Etats-membres et les institutions de l'Union Européenne ont tous recours à l'archivage en ligne permanent (*permanent on line archive*), pour la législation comme pour les décisions des cours et tribunaux.

Le recours à des solutions compatibles avec les standards d'internet (XML notamment) pour faciliter l'accès des citoyens aux données conservées est donc une priorité.

1.1. Le Journal Officiel français et le site Legifrance *(The french « Journal Officiel » and the website Legifrance)*

En France, l'accès en ligne est assuré sur deux sites officiels :

- une version électronique authentique sur le site du Journal Officiel ;
- une version électronique non certifiée sur le site Legifrance.

- Le site du « Journal Officiel de la République Française » :

Les textes publiés au Journal Officiel sont produits sous forme de fichiers PDF, avec un sommaire en XML.

L'archivage est assuré de la manière suivante :

- sur le site du Journal Officiel ne sont conservés que les textes authentifiés numériques d'origine (born digital). *Les textes antérieurs à la version électronique sont scannés et diffusés sur DVD depuis 1940, sans certificat. La numérisation du stockage antérieur se poursuivra jusqu'aux textes en vigueur les plus anciens.*

- l'archivage des textes juridiques certifiés authentiques a lieu par le gravage et l'envoi mensuel de DVD aux Archives Nationales (avec signature électronique). *Y sont stockés les fichiers et les journaux (log) où sont conservés les historiques des documents (interventions, incidents, signatures (identité des signataires, date et heure) etc.*

- le dépôt légal du support Internet du Journal officiel est effectué à la Bibliothèque Nationale de France (BNF). *C'est une obligation comme pour toute publication éditée, dans le but non pas de conserver le document authentique mais de constituer une mémoire patrimoniale. Elle est effectuée par un robot, mais sans vérification de signature électronique.*

- Le site Legifrance

Sur Legifrance, il ne s'agit pas d'archivage à proprement parler : le site n'assure qu'un simple stockage et met à disposition, à des fins de recherche documentaire, l'intégralité des lois et règlements applicables quelle que soit leur ancienneté, dans

leur version d'origine mais aussi dans leur version consolidée intégrant les modifications successives des textes.

La complémentarité des deux sites est confirmée à l'usage : d'un côté le site d'archivage du Journal Officiel qui constitue en quelque sorte le « sanctuaire » où l'on va consulter la version authentique des textes en cas de doute ou de litige et d'autre part le site de stockage de la documentation juridique, Legifrance, doté d'un moteur de recherche puissant. Il est à noter que l'absence de certification des textes diffusés sur Legifrance ne freine pas les utilisateurs puisque le site a reçu 40 millions de visites en 2007.

L'archivage des données juridiques n'est bien entendu pas l'exclusivité de l'Etat : les professionnels de l'information du secteur privé, commercial ou non, ont aussi un rôle à jouer. Pour éviter des redondances coûteuses ou l'obsolescence technologique des systèmes d'archivage, un dialogue, une collaboration, un partenariat est indispensable entre ces différents acteurs (institutions émettrices des textes officiels, bibliothèques universitaires et sociétés commerciales notamment) afin de développer des standards commun de conservation des documents juridiques et de migration de ces documents pour s'adapter aux nouvelles versions de logiciels et de matériels.

1.2. Les JO européens et le site EUR-Lex *(The european legal gazettes and the portal EUR-Lex)*

La méthode retenue pour les journaux officiels en Europe est la même : intégration des documents dans une structure commune XML avant de les exporter, soit dans une base de données soit dans différentes structures XML avec un portail permettant de les retrouver grâce à un système de repérage par méta-données.

Le format PDF (*1.4 (PDF/A-1) préconisé par la norme ISO 19005 pour la conservation des données)* doit permettre à l'avenir un archivage de documents juridiques authentiques, fiables, complets, intacts et exploitables, au fil de l'évolution des multiples générations successives de supports technologiques.

Au niveau des institutions de l'Union Européenne, EUR-Lex offre un accès direct et gratuit au Journal Officiel de l'Union européenne ; cela inclut notamment les traités, la législation et ses actes préparatoires et la jurisprudence. Le contenu de la base de données, qui remonte aux origines de la Communauté européenne, comprend quelque 2 300 000 documents en plusieurs langues, dont la plupart ont été publiés au *Journal officiel de l'Union européenne* et/ou dans le *Recueil de la jurisprudence de la Cour de justice.* N'est archivée à ce jour que la vesion TIF des textes.
L'archivage de la version PDF est en cours.

Il n'y a pas de garantie qu'un document disponible en ligne reproduise exactement un texte adopté officiellement. Seul fait foi le texte publié dans les éditions papier du Journal officiel de l'Union européenne.

2) la doctrine

Pour l'archivage de la doctrine, la Bibliothèque nationale de France, avec le projet Europeana, développe un prototype de bibliothèque numérique européenne, qui contiendra notamment une part considérable de ses collections juridiques.

Elle constitue également un réseau pour assurer l'exhaustivité et la complémentarité des différents corpus existants *(des bibliothèques institutionnelles, d'universités, de groupes de chercheurs, de représentants des ministères et autres acteurs, telles que l'Assemblée nationale, le Sénat, la Cour de Cassation)* et leur interopérabilité par la multiplication des liens entre les différents portails et par le développement de partenariats nationaux et européens, pour parvenir à une harmonisation technique.

B) L'authentification de l'édition électronique des journaux officiels en Europe (*The authentication of digital legal gazettes in Europe)* :

(Source : rapport final du groupe de travail sur l'authenticité créé par le Forum européen des Journaux officiels, présenté par Aki Hietanen, Ministère de la Justice, Finlande)

Introduction

Selon l'Organisation internationale de normalisation (ISO) *(cf. la norme ISO 15489-1, Information et documentation-Records Gestion)*, un document authentique, qui fait foi, est un document dont il peut être prouvé :
1) qu'il est ce qu'il prétend être,
2) qu'il a été créé ou envoyé par la personne censée l'avoir créé ou envoyé,
3) qu'il a été envoyé ou créé au moment prétendu.

Pour assurer l'authenticité des documents numériques, il faut donc mettre en œuvre des procédures qui contrôlent leur création, leur transmission, leur réception, leur mise à disposition et leur entretien.
Ces systèmes d'authentification sont devenus une partie essentielle du commerce électronique
et du e-gouvernement sur Internet. Au niveau européen, une coopération étroite s'est donc imposée entre les Etats membres.

Dans un contexte de développement très rapide des Journaux officiels électroniques et de diminution des versions papier et de leurs abonnés, un groupe de travail sur l'authenticité a été créé par le Forum européen des Journaux officiels *(European Forum of Official Gazettes)* en Septembre 2004 à Vienne. Il a travaillé jusqu'en 2007 avec les délégations de 14 des 27 Etats-membres : l'Autriche, la Belgique, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Islande, l'Italie, la Lettonie, la Lituanie, le Portugal et l'Espagne.

1° constat du groupe de travail : il considère avant tout qu'une distinction doit être faite entre :

1) l'authenticité des documents électroniques,
2) l'authentification des processus de production de documents électroniques,

3) l'authentification de l'impression et de la livraison de documents électroniques.

2° constat : selon lui, l'authenticité ne peut être considérée comme une question isolée, mais plutôt comme une partie de la complexité du processus de publication de la législation à la fois sur papier et sous forme électronique.

Cette approche de l'authentification des actes légaux soulève à la fois des questions juridiques et des questions techniques.

1) Aspects juridiques (le statut de l'édition électronique du journal officiel)

(Legal issues (on the legal status of the digital legal gazettes).)

Le principal aspect juridique est celui du **statut de l'édition électronique du journal officiel**, qui est indissociable du statut de l'édition traditionnelle sur papier.

Cette relation entre la version électronique et la version papier pose les questions suivantes, de manière récurrente, dans les Etats-membres de l'Union Européenne :

1°) Faut-il réglementer l'ordre de publication entre la version papier et la version électronique ?

Dans la plupart des pays européens, les versions papier et électroniques sont publiées simultanément, mais dans la pratique la version électronique est naturellement disponible plus tôt que la version papier.

2°) L'entrée en vigueur de l'acte dépend-elle de la version papier ou de la version électronique ?

Traditionnellement, les actes entraient en vigueur le jour où la version papier était disponible ou quelques jours après. L'édition électronique a changé cette situation, comme on le verra plus loin: aujourd'hui, dans un certain nombre de pays (par exemple l'Autriche, la France et l'Estonie), la loi entre en vigueur le jour de sa publication sous forme électronique.

3°) Existe-t-il des lois ou des actes de droit dérivé publiés uniquement sous forme électronique ?

La réduction des coûts de l'édition électronique a contribué à une évolution récente tendant à ce que, dans certains pays, un certain nombre textes de droit dérivé ne soient publiés que sous forme électronique. Ce type de publication uniquement électronique a été utilisé par exemple en France, en Finlande et en Slovénie.

4°) Y a-t-il une clause de force majeure si la version électronique n'est pas disponible ?

La vision moderne de l'édition électronique de la législation part du principe qu'Internet fonctionne et que le piratage ne perturbe pas l'accès au droit. Toutefois, d'éventuels problèmes ont été pris en compte dans la législation de certains États membres, comme en Autriche : si la publication sur,Internet est temporairement impossible, cette publication a lieu d'une autre manière, sous forme papier, ne serait-ce qu'à titre probatoire. A noter que

la même clause existe dans certains Etats, mais pour l'hypothèse inverse où c'est la version papier qui ne paraîtrait pas.

On peut ramener à trois les conceptions qui prévalent en Europe sur la relation entre la version
papier et la version électronique :

1.1. La solution traditionnelle *(the traditional approach)*

Dans la majorité des pays, comme pour les institutions européennes, **la version papier est encore la seule authentique et juridiquement valable**, ce qui n'empêche pas de publier une version électronique non officielle du journal officiel, le plus souvent à des fins d'information et pour faciliter l'accès aux documents juridiques. Généralement, ces journaux officiels électroniques sont disponibles en format html ou pdf.

1.2. La solution équilibrée *(the balanced approach)*

Elle a fait des progrès à la fin des années 1990 dans un certain nombre de pays qui ont décidé que **la version papier et la version électronique** auraient le **même statut juridique**. Toutefois, au cas où il y a une différence dans le contenu de la version papier et de la version électronique, la version papier est généralement la seule qui fait foi.

C'est la cas en France depuis le 2 juin 2004, date à laquelle a débuté la publication quotidienne simultanée de deux versions du « Journal Officiel de la République Française », l'une sur papier et l'autre sur support électronique authentifié.

La question de la suppression de la version papier s'est posée mais son maintien a été décidé jusqu'à nouvel ordre pour trois raisons :
1) la garantie d'égalité d'accès des citoyens à la règle de droit,
2) le statut privilégié qui reste attaché au support papier dans les professions juridiques et judiciaires, malgré les progrès considérables qu'apportent les technologies, notamment au niveau de la recherche,
3) Le besoin de garantie d'authentification à long terme des textes juridiques dont les pouvoirs publics en France veulent être assurés avant de franchir ce pas.

- Exceptions :

Le principe de la publication quotidienne simultanée de deux versions du Journal Officiel, l'une sur papier et l'autre sur support électronique authentifié connaît en France deux exceptions :

En premier lieu, est exclue la publication par voie électronique de certains actes individuels relatifs notamment à l'état et à la nationalité des personnes, dans un souci de protection de la vie privée.

En second lieu et à l'inverse, dans un but d'économie de papier, certains actes ne font l'objet que d'une publication par voie électronique car ils n'intéressent pas les citoyens dans leur vie quotidienne : il s'agit notamment de ceux qui sont relatifs à

l'organisation administrative de l'Etat, aux fonctionnaires et agents publics, aux magistrats et aux militaires ainsi qu'au budget de l'Etat.

- Effets :

Le principe de la publication quotidienne simultanée de deux versions du Journal Officiel, l'une sur papier et l'autre sur support électronique authentifié a deux effets :

1) La version papier et la version électronique ont la même valeur légale, l'authenticité des deux versions étant également assurée.

2) Les textes publiés au Journal officiel entrent en vigueur le lendemain de leur publication, qu'elle soit papier ou électronique *(à condition toutefois qu'ils ne fixent pas eux-mêmes une date d'entrée en vigueur spécifique).*

- Obligations :

Le principe de la publication quotidienne simultanée de deux versions du Journal Officiel, l'une sur papier et l'autre sur support électronique authentifié, comporte deux obligations :

1) La version électronique doit présenter des garanties non seulement pour la facilité d'accès aux textes mais aussi pour leur authenticité. Cette version électronique authentique doit par ailleurs être conservée dans des conditions garantissant son intégrité. **Tant que ces conditions ne seront pas réunies de manière certaine, la version imprimée sera maintenue**.

2) Les deux versions doivent être accessibles de manière permanente et gratuite. L'obligation d'accès permanent suppose que les données juridiques électroniques ne soient pas seulement archivées de telle manière que leur intégrité soit préservée mais aussi **maintenues en ligne, à la disposition permanente des citoyens**.

Notons enfin que dans d'autres Etats membres de l'UE ayant choisi la solution équilibrée comme l'Estonie, la tendance est de privilégier progressivement la version électronique qui deviendra à terme la seule faisant foi, la version papier se ramenant à cinq copies pour l'archivage : c'est la solution du futur.

1.3. La solution du futur *(the advanced approach)*

Elle est assez récente : au cours des dernières années, un certain nombre d'Etats-membres que l'on peut dire d'avant-garde ont adopté de nouvelles règles sur les versions papier et électronique du journal officiel, déclarant **la version électronique comme la principale version authentique**. Par rapport à l'approche traditionnelle, la situation est renversée: il est possible de publier une version papier authentifiée du journal officiel, mais le plus souvent à des fins d'information et d'archivage des documents. Le nombre de ces copies papier a été limité à 4 ou 5 exemplaires.

La Belgique a été parmi les premiers pays à réduire le nombre de copies imprimées : depuis le 1° janvier 2003, *seuls cinq exemplaires sur papier de chaque « Moniteur » sont produits (pour le Ministère de la Justice, le Moniteur belge, la Bibliothèque nationale et les Archives nationales et un pour le microfilmage) à des fins d'archivage, d'accessibilité et de continuité du principe de la publication. La seule façon pour les citoyens de consulter le Journal officiel est en format PDF sur le site sécurisé du ministère fédéral de la Justice (www.moniteur.be).*

En Autriche, la publication du journal officiel a été réformé le 1° janvier 2004 *: seule la version électronique faisant foi de l' « Austrian Federal Law Gazette » est publiée dans le système d'information juridique officiel, avec la signature électronique. Il est à noter que l'éditeur officiel, qui fait face une demande importante pour une poursuite de l'édition papier, en édite une version non authentifiée.*
Des exemplaires non officiels sur papier subsistent aussi pour l'archivage: trois copies de sauvegarde et quatre imprimés certifiés doivent être faits de chaque document (Une copie de sauvegarde certifiée de chaque impression doit être déposée aux Archives nationales et à la Bibliothèque nationale d'Autriche. Une copie certifiée est transmise également à la Bibliothèque du Parlement).

En Slovénie, la même réforme a été réalisée en 2005 *: le journal officiel est publié sous forme électronique et en version imprimée. L'édition électronique officielle, avec signature électronique sécurisée, est publiée sur le site Web public. L'édition électronique et la version imprimée sont publiées le même jour. Lorsque les deux éditions ne sont pas publiées le même jour ou ne contiennent pas le même texte, l'édition électronique prime.*

Au Portugal, une nouvelle loi relative au journal officiel est entrée en vigueur le 1° juillet 2006 *pour modifier son organisation, son entrée en vigueur et sa distribution : Le Diário da República a été ramené de trois à deux séries, la version électronique devenant la version faisant foi. Depuis, les actes ne deviennent officiels qu'après leur publication sur le site web public (www.dre.pt). La version papier a été abandonnée le 31 Décembre 2006.*

Au Danemark, l'automatisation de tout le processus de production a été réalisée le 1°janvier 2008, date à laquelle la seule version électronique du journal officiel a été maintenue.

En Espagne, on annonce la même réforme pour l'an prochain.

2) Aspects techniques *(Technical issues)*

Le principe de la publication quotidienne simultanée de deux versions du Journal Officiel, l'une sur papier et l'autre sur support électronique authentifié pose aussi des questions techniques relatives à la réorganisation et à la sécurisation des systèmes de production et de diffusion des Journaux Officiels.

En amont de la conservation de la version électronique, sa mise en ligne, qui joue un rôle d'authentification analogue à la publication de l'édition imprimée, doit présenter des garanties particulières de sécurité. C'est pourquoi une chaîne de confiance doit être établie permettant d'authentifier la source émettrice des publications officielles. L'acte d'authentification est matérialisé par une clé de certification faisant figurer la date et l'heure de publication ainsi que l'origine de la certification.

Si l'on y ajoute les aspects techniques liés à l'authentification du document lui-même par la signature électronique, on constate que l'on impose à la publication électronique des actes des contraintes d'authentification qui n'ont jamais été imposées à la publication imprimée sur papier.

2.1. La signature électronique *(digital signature)*

Une signature électronique est utilisée pour authentifier l'identité de l'expéditeur d'un message ou du signataire d'un document. Elle est également utilisée pour assurer l'intégrité du contenu original d'un document ou d'un message.

Le texte de base dans l'UE est la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques. Elle définit une signature électronique comme: "des données sous forme électronique jointes ou liées logiquement à d'autres données électroniques et qui servent de méthode d'authentification de celles-ci".

2.1.1. Les trois formes de signature électronique

1) la signature électronique simple *(simple signature)*
2) la signature électronique avancée *(advanced signature)*
3) la signature électronique qualifiée *(qualified signature)*

1) la signature électronique simple :
Il lui est donné un sens large. Elle sert à identifier et authentifier les données. Elle peut être aussi simple que la signature d'un e-mail avec le nom d'une personne ou l'utilisation d'un code PIN.

2) la signature électronique avancée :
Elle appartient uniquement au signataire et doit être capable de l'identifier; elle est créée par des moyens que le signataire doit pouvoir garder sous son contrôle exclusif ; bien entendu, elle est liée aux données auxquelles elle se rapporte.

La directive européenne est neutre sur le plan technologique, mais dans la pratique, cette définition se réfère principalement aux signatures électroniques basées sur une infrastructure à clé publique (ICP). Cette technologie utilise une technologie de cryptage des données à signer.

3) la signature électronique qualifiée :
Il s'agit d'une signature basée sur un certificat qualifié et créée par un dispositif sécurisé de création de signature, dispositif devant satisfaire aux exigences énoncées aux annexes de la directive européenne.
Un exemple de l'utilisation de la signature électronique qualifiée se trouve dans la base de données autrichienne de la législation authentique (BGBL Autentisch), où il y a quatre formats: HTML, PDF, Word et authentique texte XML : la signature numérique peut être consultée et vérifiée dans chaque format.

2.1.2. Les normes de signature électronique *(digital signature standards)*

Aujourd'hui, il existe un grand nombre de normes de signature électronique ; retenons les deux suivantes :

1) XAdES (norme ETSI européenne).

La norme européenne *(ETSI TS 101 733 de)* XAdES définit les formats pour les signatures électroniques avancées, qui restent valables sur de longues périodes, sont conformes aux exigences de la directive européenne et permettent d'intégrer d'autres informations utiles.

Une signature électronique produite conformément à la norme XAdES apporte la preuve que certains engagements ont été explicitement approuvés dans le cadre d'une stratégie de signature, à un moment donné, par un signataire doté d'un identifiant (un nom ou un pseudonyme et éventuellement une fonction).

2) Signature électronique de documents PDF

Le logiciel Adobe Acrobat contient un certain nombre de normes en matière de signature électronique, en particulier les normes dites PKCS. La meilleure façon de découvrir qu'un document PDF est authentique et véritable est de vérifier les signatures numériques qu'il contient : immédiatement après l'ouverture d'un document Adobe PDF certifié, le logiciel Adobe Reader ou Acrobat vérifie automatiquement les modifications non autorisées au document et vérifie l'authenticité de la signature de certification.
Un document PDF peut avoir deux types de signatures numériques, une signature de certification, qui peut être appliquée par l'auteur du document, et une signature appliquée par toute personne qui a la permission de signer numériquement le document.
Adobe Reader ou Acrobat vérifie automatiquement l'authenticité de ces signatures lorsqu'on ouvre le document, puis affiche une fenêtre qui indique que la signature est valide c.a.d. authentique et actuelle.

2.1.3. Les défis dans l'utilisation des signatures électroniques *(challenges in the use of digital signatures)*

Il y a plusieurs défis dans l'utilisation des signatures électroniques :
- Le premier défi réside dans le **choix des signatures les plus appropriées**. Il existe plusieurs solutions de rechange et des procédures différentes pour l'utilisation de chacune d'entre elles.
- Le deuxième défi pour les signatures électroniques est le vieillissement, la **limitation dans le temps de leur validité**, qui pose le problème de la conservation à long terme de versions authentifiées : l'augmentation de la puissance de calcul, les possibilités de mise en réseau et les progrès de la cryptographie contribuent à l'"affaiblissement" des signatures électroniques, les documents signés électroniquement pouvant perdre leur valeur probante au fil des ans. Le défi du renouvellement de signature reste important pour les années à venir.
- Le troisième défi est lié à la **réforme et au transfert de données.** Les signatures électroniques peuvent être brisées lors du changement de format des documents. Le développement technologique, les tentatives d'harmonisation, et aussi de nouvelles directives juridiques entraînent des modifications des données relatives à l'utilisateur et des formats de signature au fil des ans. Avec les documents signés électroniquement, des modifications de format sont problématiques, car la

modification du format rompt la signature originale. Mais on peut dire qu'un problème similaire se pose au cours de la numérisation des documents papier : si, par exemple, un document signé à la main est numérisé, la signature perd sa validité. L'authenticité juridique du document ainsi transformé devient douteuse.

2.1.4. Les pratiques des Etats membres de l'UE *(pratices in the member States of the EU)*

De nos jours les signatures électroniques ne sont utilisées pour les Journaux Officiels que dans un petit nombre de pays : l'Autriche, la France, la Grèce et la Slovénie.

En France, il existe deux types de signatures électroniques utilisées dans la chaîne de confiance.
XAdES est utilisé dans la plupart des cas au plus haut niveau d'authentification, mais aussi la signature PDF (PKCS).

En Autriche, une signature numérique basée sur XML est utilisée depuis 2004. Les documents qui quittent le flux de travail sécurisé sont signés électroniquement sur une base XML, en utilisant XML-DSIG.

2.2. Le flux de travail, la chaîne de production et la chaîne de confiance *(Workflow, production chain and chain of confidence)*

Le flux de travail est lié au processus électronique de gestion des actes : il traite les validations et la priorité de l'ordre dans lequel ils sont présentés ; il en assure l'intégrité de la première ébauche jusqu'au texte final publié au JO.
La chaîne de confiance est un processus fiable de production de documents électroniques authentifiés par les signatures électroniques. Des méthodes de diagnostic et de vérification de l'intégrité du processus interviennent dans les différentes phases.
La chaîne de confiance peut ne couvrir qu'une partie du processus de production, par exemple les dernières étapes de la préparation de la publication des actes reçus des ministères et du Parlement.

Encore peu de pratique dans les Etats membres de l'UE :

En France, une chaîne de confiance a été créée en amont du processus de publication, dans le but d'authentifier la version électronique du Journal officiel.

Le système dénommé S.O.L.O.N (Système d'Organisation en Ligne des Opérations Normatives) a pour objet de dématérialiser une grande partie du processus d'élaboration, de vérification et d'approbation des textes à publier au Journal officiel. Il vise à doter l'ensemble des institutions associées à la production de ces textes d'une application commune capable de prendre en charge les projets sous format numérique, d'en assurer le transport au cours des étapes successives, et de les remettre à la direction des Journaux officiels sous la forme d'un flux XML structuré.

L'application garantit la traçabilité de chacune des étapes du parcours des projets ainsi que la conservation de leurs états successifs, ce qui concerne quelques 30 000 textes par an. Environ 500 personnes seront contributeurs de l'application au sein

de l'ensemble des institutions précitées (La présidence de la République, le secrétariat général du Gouvernement, la direction des Journaux officiels, les ministères, le Conseil d'Etat, les autorités administratives indépendantes et certaines instances consultatives).

Pour rendre possible et efficace le travail interministériel au moyen de S.O.L.O.N, il est nécessaire de respecter, dès les premières étapes de rédaction des projets, un standard commun de présentation des textes. Les projets doivent être disponibles sur le format MS Word (cette prescription pourrait être modifiée lorsque les ministères auront achevé le déploiement, sur leurs réseaux, d'outils bureautiques libres) ; ils doivent en outre respecter les modèles (ou feuilles de style) proposés par l'application. La fonction de signature et de contreseing électroniques des actes n'entre pas dans le cadre actuel du projet, mais pourrait être prise en compte au cours d'une phase ultérieure.

En Autriche, le projet e-Recht concerne différents flux de travail pour les ministères et pour le Parlement, pour les lois, les règlements et les traités. Les documents sont écrits en MS Word et convertis en XML.

Au Portugal, un système nommé RedeLex est en cours de démarrage. C'est est le réseau électronique de la procédure législative. Ce projet permet l'interconnexion, d'une manière sûre et privée, des institutions de l'Etat qui participent à la procédure législative électronique (le gouvernement, la présidence de la République, l'Assemblée de la République et la Cour constitutionnelle). Il établit un lien entre ce réseau et le Secrétariat général de la présidence du Conseil des ministres et l'Imprimerie nationale. RedeLex utilise les signatures électroniques qualifiées et garantit la sécurité de la transmission de données.

En Finlande, un système appelé PTJ est le réseau électronique de procédure législative. Le premier PTJ a été créé en 1995 et le nouveau PTJ2 a été introduit en 2005 ; il utilise le logiciel Documentum. Les projets de loi sont transférés, au sein du système, des ministères au gouvernement et au Parlement en format XML structuré. L'outil pour la rédaction proprement dite est MS Word, avec des modèles sur mesure et des macros.

Les bonnes raisons et les limites du recours au workflow :

Les bonnes raisons :

1) La dématérialisation a des effets directs : immédiateté / fiabilité des transmissions ; gain de temps dans le chaînage des opérations ;

2) Elle a des effets induits : meilleures possibilités d'archivage, vérifications facilitées, consultation à tout moment des états antérieurs ;

3) Elle ouvre la possibilité de produits dérivés : tableaux de bord, états de synthèse divers ;

4) Elle conduit nécessairement à s'interroger sur la répartition des responsabilités et peut amener à simplifier la chaîne hiérarchique ;

5) Elle contribue à l'amélioration de la qualité de la réglementation ;

6) Elle facilite le travail de publication au Journal Officiel papier et électronique.

Les limites :

1) Il n'est ni souhaitable, ni possible de tout dématérialiser : les échanges verbaux et les contacts téléphoniques, par exemple, doivent pouvoir être maintenus;

2) Tous les cas particuliers ne sont pas nécessairement à répertorier ni à prendre en compte ;

3) Certaines étapes de la procédure échappent à la dématérialisation : Conseil d'Etat, assemblées parlementaires, organismes consultatifs ;

4) La reprise de l'existant n'est pas envisageable ;

5) L'analyse juridique échappe par nature à l'application : dématérialiser les procédures ne signifie pas les automatiser.

Quelques recommandations pour la modification de la chaîne de production du J.O. afin de la rendre aussi sûre que possible :

1) Réorganisation d'abord de la chaîne de production avec :

- une gestion parallèle de deux circuits de publication et de deux logiques de fabrication ;
- un contrôle de cohérence des contenus ;
- une publication de deux éditions avec sommaire commun et typographie adaptée ;
- la production d'un fichier PDF par texte, d'un sommaire en format PDF et XML et d'un fichier PDF avec l'ensemble des textes et le sommaire.

2) Vérification des possibilités d'utilisation du flux de travail et de la chaîne de confiance

- essayer de minimiser le nombre de flux de travaux ;
- commencer avec une chaîne de confiance de portée limitée ;
- explorer les possibilités d'utiliser les éléments génériques (cf. les éléments génériques autrichiens : modules pour les applications en ligne) pour la vérification de signature, l'identification et la fourniture de documents ;
- examiner les possibilités d'utiliser les logiciels standard et générique de traitement de texte des applications et des normes (par exemple DigiDoc).

2.3. Les serveurs sécurisés et les certificats pour l'édition
(Secure servers and certificates in the delivery of digital legal gazettes)

Troisième aspect technique quant à la garantie d'authenticité des actes électroniques : l'utilisation de serveurs et de protocoles sécurisés pour la production électronique des J.O. Elle permet d'assurer la fiabilité de tout document électronique source et de tout transfert de données depuis le serveur.

Un serveur sécurisé est un serveur web qui prend en charge un protocole de sécurité qui chiffre et déchiffre des messages afin de les protéger contre la falsification des tiers. *Les principaux protocoles de sécurité sont SSL, SHTTP (Secure HTTP), et IPSec (Internet Protocol Security).*
Il assure des connexions sécurisées et le cryptage des données dans le processus de transit entre l'utilisateur et le serveur.

Lors d'une connexion SSL cryptée, toutes les données sont transmises entre un client et un serveur pour être cryptées par le logiciel d'envoi et déchiffrées par le logiciel de réception, garantissant la protection des renseignements personnels contre toute interception sur Internet. En outre, toutes les données envoyées via une connexion SSL cryptée sont protégées par un mécanisme de détection de l'altération destiné à déterminer automatiquement si les données ont été modifiées en cours de transit.

Pratiques dans les Etats membres de l'UE :

En France, un serveur sécurisé avec certificat est utilisé par le Journal Officiel.
Le dispositif de sécurité est le suivant:

- *génération de trois certificats avec trois autorités de certification (racine, serveur, utilisateur) et un certificat de signature ;*
- *validation par les personnes habilitées avant la signature ;*
- *signature au standard XAdES (signature électronique XML) ;*
- *sécurité de l'accès sur le site du Journal Officiel avec vérification de signature (Applet java, ActiveX) mais possibilité d'accès sans vérification*
- *accès sur le site Legifrance : possibilité d'accès à des fichiers PDF non signés*

Au Portugal comme en Estonie, un certificat de serveur HTTPS Web a été créé pour le Journal Officiel ; il intègre un certificat (Multicert au Portugal, Thawte en Estonie) qui garantit la validité.

Recommandations sur l'utilisation de serveurs sécurisés et de certificats :
- Vérifier et garantir la protection physique des bases de données documentaires et de contrôle d'accès aux bases de données originales (pare-feu etc)
- Mettre en place un serveur sécurisé par ex avec protocole https. Activer les certificats SSL sécurisés.
- Utiliser des serveurs sécurisés avec architecture ouverte pour une réduction des coûts. *Par ex Plone est un prêt à terme système de gestion de contenu qui se construit sur la libre serveur d'applications Zope. Zope est un Open source web serveur d'applications, avec une base de données transactionnelle objet qui peut également stocker des modèles HTML dynamique, des scripts, un moteur de recherche et de bases de données relationnelles (SGBDR) et le code connexions.*
- Utiliser le serveur open source de logiciels d'applications, par exemple Apache SSL.

Conclusion :

D'une manière générale, on a actuellement tendance à imposer aux données juridiques électroniques des contraintes de certification trop lourdes, d'autant qu'on n'en demande pas aux éditions imprimées.

Par conséquent, il est nécessaire d'évaluer les coûts et les avantages des différentes techniques et méthodes et de consulter les utilisateurs des services pour analyser leurs besoins pratiques.

En France, une enquête menée auprès des utilisateurs a montré que l'authentification des textes officiels diffusés sur support électronique n'était pas du tout une priorité pour eux et que les problèmes techniques qu'ils pouvaient rencontrer pour afficher un certificat en ligne ne constituait pas un frein à leurs recherches. En effet, il ne semble pas que la diffusion de textes non certifiés sur Legifrance soit dissuasive puisque le site a reçu quarante millions de visites en 2007. On constate que l'authenticité est le plus souvent présumée par les usagers dès lors que la diffusion est assurée par un site «.gouv ».

Expérience similaire dans d'autres Etats membres de l'UE où très peu d'utilisateurs ont effectivement utilisé la possibilité de confirmer l'authenticité du J.O. électronique :

En Hongrie, l'authentification avec un logiciel spécifique peut être difficile, voire impossible, sur certains postes de travail, si l'utilisateur n'est pas autorisé à installer le logiciel.

En Autriche, actuellement 51% utilisent la version pdf du J.O., 36% utilisent la version html, 11% utilisent la version Word et seulement 2,3% utilisent la version authentique, qui intègre la signature électronique.

Il y a un peu des résultats similaires du Portugal : la version électronique qui fait foi depuis Juillet 2006 est accessible via un système sécurisé, en utilisant HTTPS, et un système non sécurisé. Actuellement, seuls environ 7% utilisent le système sécurisé.

Les exigences des utilisateurs vont en priorité vers la qualité rédactionnelle des textes et leur accessibilité : l'accès à des textes compréhensibles et à jour doit donc être un objectif prioritaire pour les pouvoirs publics, même si la question de leur authentification ne doit pas être négligée pour autant.