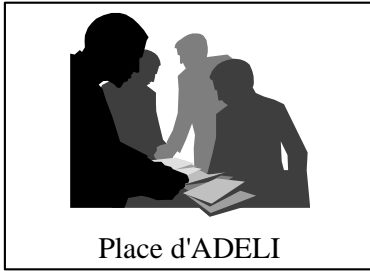




# ADELI

La LETTRE n° 49

Octobre 2002



# www.adeli.org

## **Nouveau site Web pour ADELI Histoire d'une refonte**

*Si vous aviez l'habitude de consulter le site d'Adeli à l'adresse <http://www.adeli.com>, vous avez peut-être remarqué que vous étiez automatiquement redirigé vers <http://www.adeli.org>. La page d'accueil que vous y découvrirez est presque identique à celle que vous connaissiez, en y regardant de plus près vous remarquerez cependant de nombreux changements, qui appellent des commentaires.*

*Cet article a pour objectif de vous exposer notre démarche, en espérant qu'elle pourra vous servir dans l'administration de vos sites professionnels, associatifs ou personnels.*

## **Pourquoi changer ?**

Notre site était tout à fait présentable depuis qu'il avait adopté les couleurs bleu et blanc de la charte graphique ADELI et que l'un des membres du Comité, Prasong Cuong Kham, avait conçu une page d'accueil au graphisme subtil. Le nombre de visiteurs augmentait d'ailleurs régulièrement. Nous aurions pu nous satisfaire encore quelque temps de cette situation.

Quelques points laissaient cependant à désirer :

- Nous n'avions pas réussi à faire décoller l'espace adhérent ni les forums qui y étaient cachés ;
- Les informations sur la vie de l'association et plus particulièrement des commissions n'étaient pas toujours de la dernière fraîcheur ;
- Certaines pages du site n'étaient consultables qu'au prix d'un temps de réponse assez aléatoire ;
- Le site souffrait, globalement, d'un manque d'interactivité et d'une fréquence insuffisante des mises à jour ;
- Enfin, considération très égoïste, la charge de travail du webmestre<sup>1</sup> était lourde et quasiment impossible à répartir entre plusieurs adhérents, pourtant volontaires...

Une première évolution majeure avait consisté à rendre dynamique l'accès et la consultation des articles anciens de la lettre, via une base de données MySQL<sup>2</sup>, accessible par un script PHP<sup>3</sup>. Pour disposer de ces fonctionnalités, non offertes par notre hébergeur payant, nous avons dû loger notre base de données chez Free, hébergeur gratuit, connu de tous les internautes. Ceci explique d'ailleurs les temps de réponse quelquefois assez longs que vous subissiez lors de la recherche d'un article.

Nous avons également expérimenté la fonction forum chez Free, en installant des scripts PHP, récupérés en open source<sup>4</sup> sur Internet<sup>5</sup>. Rien à dire sur les fonctionnalités, mais les temps de réponse restaient désastreux.

---

<sup>1</sup> Vous l'aurez compris, c'est de moi qu'il s'agit !

<sup>2</sup> MySQL est un système de gestion de bases de données relationnelles, développé en Open Source. **MySQL** utilise la licence GPL (GNU General Public License). Le sigle SQL, qui fait partie du nom **MySQL**, signifie "Structured Query Language" (Langage Structuré de Requête) - c'est le langage le plus répandu pour accéder aux bases de données.

<sup>3</sup> PHP (officiellement "PHP: Hypertext Preprocessor") est un langage de programmation, spécialisé dans la génération de code, dont le domaine de prédilection est HTML. Il fonctionne côté serveur.

<sup>4</sup> La notion d'open source implique le libre redistribution du logiciel, Pour une définition plus complète on se reportera à <http://severino.free.fr/archives/copieslocales/tribunelivre/fr-x2548.html>

<sup>5</sup> <http://www.phorum.org>

## Un nouveau nom de domaine

### *.com ou .org, qu'est-ce que cela change ?*

Com, abréviation de 'commercial', est réservé en principe aux sites commerciaux.

Org, abréviation de 'organisation', convient aux associations et autres organismes à but non lucratif.

Selon que votre site sera nommé en .com ou .org, il sera référencé différemment par les moteurs de recherches et annuaires divers qui attirent les visiteurs et conditionnent le nombre de visiteurs. J'ai du essayer le refus d'indexation de plusieurs moteurs de recherches, lié à l'étiquette commerciale qu'ils nous attribuaient.

Nous avons fait le choix d'acquérir le nom de domaine adeli.org, sans toutefois abandonner adeli.com.

Ces deux noms de domaines pointent sur une unique version de notre site.

## Un nouvel hébergeur

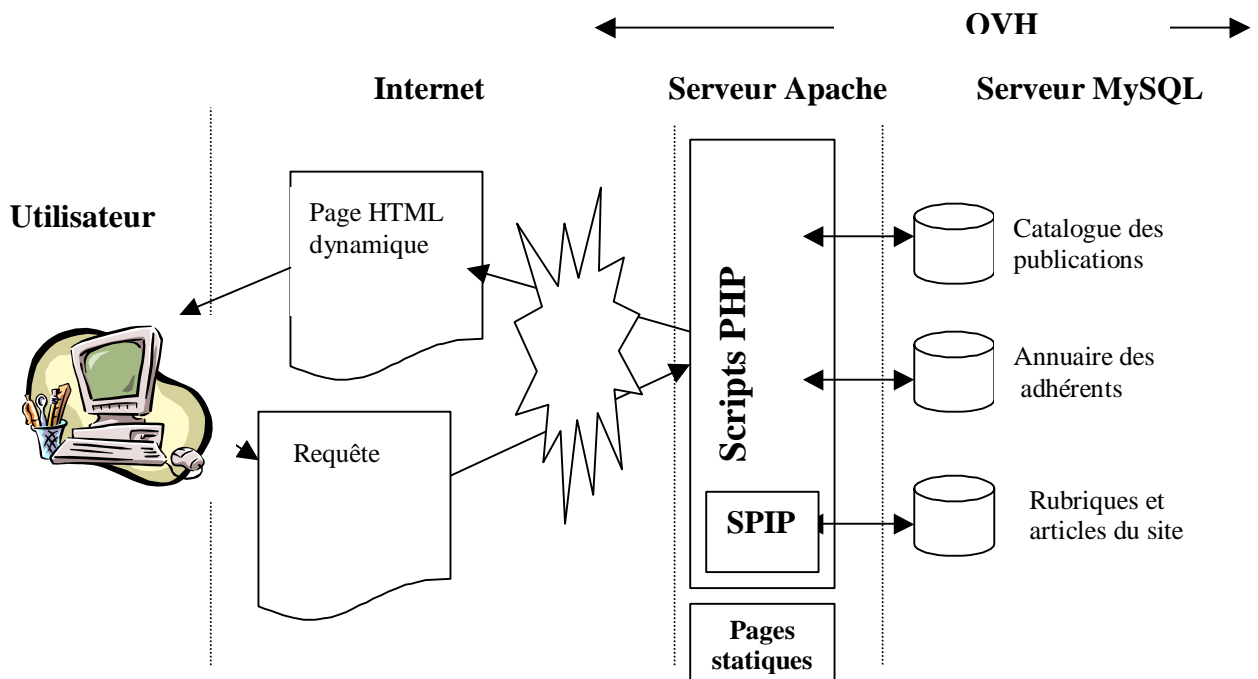
Le second choix à effectuer était celui d'un hébergeur, nous permettant l'utilisation des outils de gestion dynamiques dont nous avons besoin, à savoir PHP et MySQL.

Nos critères étaient simples et peu originaux :

- Présence des fonctionnalités requises pour le développement d'un site dynamique ;
- Prix inférieur ou égal à celui de notre précédent hébergeur ;
- Performances en matière de temps de réponse et disponibilité du service.

Une comparaison rapide des offres disponibles<sup>6</sup> et appréciations des utilisateurs nous amena au choix d'OVH<sup>7</sup>, qui répondait à l'ensemble de nos critères.

## Une nouvelle architecture



Un petit schéma vaut mieux qu'un long discours....

<sup>6</sup> Un classement des hébergeurs est actualisé chaque semaine sur le site <http://solutions.journaldunet.com/dossiers/hebergement/>

<sup>7</sup> <http://www.ovh.com>

## Site statique

Notre premier site historique, construit par Jean-Luc Blary, se présentait sous une forme entièrement statique : chaque page était constituée d'un ensemble de balises HTML, codées « en dur » par le webmestre via un éditeur de texte classique (Notepad par exemple) ou un peu plus sophistiqué, tel que HotmetalPro ou FrontPage, pour bénéficier des fameuses fonctionnalités Wysiwyg<sup>8</sup>.

La moindre modification entraînait donc le cycle suivant :

- Modification sur le poste de travail du webmestre du fichier html ;
- Visualisation de l'effet rendu avec Internet Explorer et Netscape (cela peut-être très différent, et varier d'une version à l'autre) ;
- Téléchargement du fichier sur le serveur du fournisseur d'accès, via FTP ;
- Nouveau contrôle visuel.

## Site dynamique

Un site est dit « dynamique » lorsque toutes les pages HTML ne sont plus codées en dur par le webmestre, mais qu'au moins certaines d'entre elles sont générées sur le serveur par un script<sup>9</sup> qui va chercher si nécessaire les informations dont il a besoin dans des bases de données.

Suivant ce principe de séparation des données et des traitements, la dynamique du site ADELI est d'abord assurée par la mise en place de deux bases de données :

- Une base des publications qui contient la description des articles de la Lettre (depuis le N°21) : titre, auteur, résumé (quelquefois en anglais et en espéranto), mots-clés ;
- Une base des adhérents.

Ces deux bases de données peuvent être mises à jour directement par les administrateurs habilités : Alain Coulon et moi-même.

De façon encore plus radicale, la séparation entre les informations et leur mise en page a été rendue possible par l'utilisation de SPIP, Système de Publication pour l'Internet, dont nous allons maintenant vous dire quelques mots.

## SPIP et la publication en ligne

Le « bouche à oreille » fonctionne très bien dans le monde associatif et dans celui de l'Internet. J'ai ainsi découvert SPIP au hasard d'une discussion, lors d'un dîner organisé par l'AILF. Quelques jours plus tard, j'avais avec l'aide de mon fils monté un premier site expérimental sur Free et pu expérimenter les fonctionnalités fabuleuses permises par ce système.

SPIP, Système de Publication pour l'Internet, est constitué d'un ensemble de fichiers, installés sur le serveur Web, qui permettent de bénéficier d'un certain nombre d'automatismes :

- gérer un site à plusieurs ;
- mettre en page les articles sans avoir à taper de code HTML ;
- modifier très facilement la structure du site...

SPIP permet de fabriquer et de tenir un site à jour, grâce à une interface très simple d'utilisation, accessible au travers d'un simple navigateur (Netscape, Microsoft Explorer, Mozilla, Opera...).

L'intérêt principal de ce système dans un contexte associatif est de permettre la séparation et donc la répartition des tâches :

- composition graphique, qui peut évoluer sans reprise des contenus éditoriaux ;
- contribution rédactionnelle par la proposition d'articles et de brèves ;
- gestion éditoriale du site, qui comprend l'organisation des rubriques, la validation des articles proposés, l'administration des forums...

SPIP est gratuit, son code est ouvert et il est distribué sous la Licence publique générale GNU<sup>10</sup>.

---

<sup>8</sup> *What you see is what you get*

<sup>9</sup> *Le site ADELI utilise des scripts PHP, dont le principal avantage est d'être un logiciel libre ne nécessitant donc aucun investissement, disponible dans les mondes Unix, Windows et Macintosh. Un grand nombre d'hébergeurs Internet permettent aujourd'hui l'utilisation de scripts PHP.*

D'autres systèmes de publication existent. Un des plus connus actuellement est phpNuke, qui impose une structure assez rigide pour le site, sous forme de portail muni de courts articles.

SPIP est plus souple, et orienté vers la création d'un site structuré comme un magazine, avec des rubriques, sous-rubriques (et ainsi de suite), dans lesquelles sont insérés des articles et des brèves qui peuvent être complétés de forums de discussions.

Pour en savoir plus, je vous encourage fortement à consulter le site des développeurs de SPIP<sup>11</sup> : <http://www.uzine.net> où vous trouverez d'autres informations passionnantes.

### **L'arborescence du site ADELI**

Le tableau suivant vous présente la liste des rubriques et articles qui constituent actuellement le site d'ADELI. Cette structure très souple pourra être modifiée selon les besoins ; de nouvelles rubriques et sous-rubriques pourront être facilement créées lors de l'ouverture d'une nouvelle commission.

<b>Rubriques et articles gérés sous SPIP</b>			
<b>Rubrique</b>	<b>Sous-Rubrique</b>	<b>Articles publiés</b>	<b>Accès</b>
<b>Vie d'ADELI</b>		<ul style="list-style-type: none"> <li>➤ Annuaire</li> <li>➤ Contacts</li> <li>➤ Assemblée générale 2001</li> <li>➤ Conférence de l'assemblée générale</li> <li>➤ Dîner-débat du 20 juin 2001</li> <li>➤ Assemblée générale 2000</li> </ul>	Réservé adhérents L'annuaire est géré hors SPIP dans une base MySQL.
	<b>Actualités</b>	<ul style="list-style-type: none"> <li>➤ Les prochaines réunions du comité d'ADELI</li> <li>➤ Assemblée générale 2002</li> <li>➤ Assises 2002</li> </ul>	Public Rubrique mise à jour par les membres du comité. Des brèves sont associées à cette rubrique.
<b>Présentation d'ADELI</b>		<ul style="list-style-type: none"> <li>➤ Présentation d'ADELI</li> <li>➤ Les valeurs permanentes d'ADELI</li> <li>➤ Le Comité 2002</li> </ul>	Public Rubrique institutionnelle qui ne devrait être mise à jour qu'une fois par an, à l'occasion de l'AG
	<b>Notre histoire</b>	<ul style="list-style-type: none"> <li>➤ 1978-1980 - La genèse d'ADELI - La Logique Informatique</li> <li>➤ 1980-1990 - L'ouverture, la diversification et la croissance</li> <li>➤ 1991-1996 L'association française de génie logiciel</li> <li>➤ 1997-... - En avant ... vers la maîtrise des systèmes d'information</li> <li>➤ Les principaux contributeurs d'ADELI</li> </ul>	Public

<sup>10</sup> GNU General Public License ou G.P.L. Sur GNU on pourra consulter l'article BSA ou GNU ? Protection et liberté des logiciels paru dans la Lettre n°41.

<sup>11</sup> Encore merci à eux !

<b>Rubriques et articles gérés sous SPIP</b>			
<b>Présentation des commissions</b>		➤ Charte des commissions	Public Rubrique Mise à jour par les responsables des commissions
	<b>Maîtrise des processus</b>	➤ Appel à commission ➤ Programme des assises 2002	Public
	<b>Management des risques</b>	➤ Appel à commission	Public
	<b>Outils de gestion de configuration</b>	➤ Présentation de la commission	Public
	<b>Qualité et maîtrise des SI</b>	➤ Appel à commission	Public
	<b>Sécurité</b>	➤ Appel à commission	Public
<b>Publications</b>		<ul style="list-style-type: none"> <li>➤ Valeuroscope2000</li> <li>➤ AGLoscope98</li> <li>➤ AGLoscope98 - extraits</li> <li>➤ REALiscope98</li> <li>➤ REALiscope98 – le making-off</li> <li>➤ PERILoscope97</li> <li>➤ AGLoscope97</li> <li>➤ ISO 9001 et développement du logiciel – guide d'application</li> <li>➤ AGLoscope 96</li> <li>➤ AGLoscope95</li> </ul>	Public Articles créés à l'occasion des nouvelles publications
<b>La lettre</b>		➤ La lettre	Liens vers la liste des articles en ligne, téléchargeables pour ceux datant de plus d'un an.
<b>Travaux des commissions</b>			Réservé adhérents Rubrique Mise à jour par les responsables des commissions
	<b>Outils de gestion de configuration</b>	<ul style="list-style-type: none"> <li>➤ Réunion du 19 mars 2002</li> <li>➤ Réunion du 5 février 2002</li> <li>➤ Réunion du 14 décembre 2001</li> </ul>	Réservé adhérents

<b>Autres pages du menu</b>	
<b>Recherche</b>	Recherche sur mot-clé sur l'ensemble des articles du site et de la lettre.
<b>Glossaire</b>	Liste de mots clés : À chaque mot-clé sont associées une définition et la liste des articles du site ou de la Lettre pointant sur ce mot clé
<b>Liens</b>	Quelques liens utiles : <ul style="list-style-type: none"> <li>➤ Sites Internet des associations amies</li> <li>➤ Sites des adhérents</li> </ul>
<b>Pages hors SPIP</b>	<ul style="list-style-type: none"> <li>➤ Bon de commande : l'envoi d'un bon de commande en ligne à notre secrétaire devra simplement être confirmé par l'envoi d'un chèque.</li> <li>➤ Formulaire d'adhésion : un simple formulaire à imprimer et renvoyer par courrier postal à l'adresse d'ADELI, accompagné du règlement par chèque.</li> </ul>

### **Comment contribuer ?**

Une contribution directe à la vie du site est possible par l'utilisation des forums associés à chaque article. Ces forums sont actuellement modérés (prudence oblige), vos contributions seront donc mises en ligne avec un délai de quelques heures.

Un nom d'utilisateur et un mot de passe seront attribués aux adhérents souhaitant contribuer à la rédaction d'articles : Pour ce faire, envoyez un mail à [postmaster@adeli.org](mailto:postmaster@adeli.org).

***Martine Otter***  
***Présidente et webmestre d'Adeli***



Square des Utilisateurs

# Transformation vers une informatique adaptable

*L'évolution des architectures et des systèmes propriétaires vers des architectures et des systèmes ouverts autour des services web va permettre aux entreprises leur reconfiguration rapide et l'utilisation de services extérieurs fournis par d'autres entreprises.*

*Cette évolution modifiera profondément la définition, la mise en œuvre et la gestion des architectures et des systèmes d'information en permettant la création d'une informatique adaptable. Les entreprises qui redéfiniront leur stratégie et leur architecture informatique pour mettre en place cette informatique adaptable amélioreront sensiblement leur compétitivité et leurs capacités de réaction. Elles pourront ainsi satisfaire aux exigences d'évolution : adaptation aux aléas du marché, collaboration avec leurs clients et fournisseurs, coopération et compétition avec leurs partenaires et concurrents, amélioration de la qualité de leurs produits et de leurs services, et génération de nouveaux revenus.*

## Les problèmes actuels des systèmes d'information

Jusqu'à présent, l'entreprise a eu tendance à construire son système d'information par juxtaposition d'outils spécifiques. Son système se compose généralement d'applications sur mesure développées en interne et d'applications paramétrées et, très souvent, adaptées, achetées à des fournisseurs et qui doivent ensuite être configurées.

La plupart des applications actuelles sont construites comme des entités indépendantes. Elles n'ont pas été conçues comme des ensembles de services réutilisables dotés d'interfaces bien définies. Elles sont fermées et limitées dans leur capacité à s'adapter rapidement à une évolution quelconque des processus ou des besoins métier. Les processus métier sont intégrés aux systèmes propriétaires existants. Les connexions et interfaces propriétaires avec les systèmes partenaires doivent être maintenues et souvent réécrites.

Après des années de développement et d'achats disparates, au coup par coup, les entreprises en sont réduites à devoir maintenir des systèmes d'information hétérogènes manquant de cohésion globale.

Les entreprises consacrent des dépenses importantes à l'intégration de leurs silos de données, de leurs îlots applicatifs et de leurs blocs de processus métier. Les investissements coûteux dans des systèmes complexes de planification des ressources de l'entreprise (ERP - Entreprise Resource Planning) tout en résolvant quelques problèmes en ont engendré de nouveaux. Les ERPs ont remplacé le compartimentage des applications et des données au prix d'une intégration néanmoins restrictive des processus métier. L'utilisation d'ERPs a parfois rendu les entreprises moins flexibles en les ancrant dans des processus métier rigides.

En conséquence, les entreprises sont actuellement dépourvues de l'infrastructure technologique qui leur permettrait de s'adapter rapidement aux évolutions de leur marché et leur offrirait l'opportunité de damer le pion, en temps réel, à leurs concurrents. Les fusions, les acquisitions, les partenariats, et les restructurations stratégiques s'avèrent de plus en plus difficiles à exécuter.

## La réponse des fournisseurs d'infrastructure e-business

Les grands fournisseurs de solutions d'infrastructures technologiques comme IBM, Sun, BEA, Oracle et Microsoft ont investi massivement dans le développement de nouvelles technologies « e-business ». Ils ont récemment réalisé des progrès importants dans l'industrialisation des technologies Internet en développant une nouvelle technologie appelée « services web ».



Leur objectif est, non seulement, de faciliter l'évolution des entreprises vers l'e-business, mais surtout d'exploiter ces nouvelles technologies pour améliorer les performances et résultats de ces entreprises.

D'autres fournisseurs plus spécialisés tels Kenamea, Flamenco, KnowNow, Grand Central, complètent les offres de ces grands fournisseurs d'infrastructures technologiques.

L'architecture de services web est un changement de paradigme. Ces services permettent 'd'exposer' des applications comme des services qui peuvent communiquer via Internet. Fondés sur des standards, ils assurent la mise en place d'architectures flexibles et ouvertes, ce que ne permettaient pas les systèmes spécifiques propriétaires. Ils facilitent l'accès à des services applicatifs sur Internet, ce qui va favoriser l'émergence d'une nouvelle génération de fournisseurs de services applicatifs sur Internet.

## Les deux solutions actuelles de services web

Les services web sont actuellement présents sous deux architectures concurrentes :

- le framework.Net de Microsoft ;
- la plate-forme J2EE (Java 2 Entreprise Edition) de Sun Microsystems.

Ces deux architectures fournissent :

- une approche standardisée et extensible pour exposer les fonctionnalités des applications ;
- une interface pour accéder aux données et effectuer des transactions avec des applications existantes à partir du web.

Dans son architecture .Net, Microsoft crée un environnement où des applications faiblement couplées peuvent « se découvrir » automatiquement et s'intégrer l'une avec l'autre en utilisant des services web.

L'approche de Sun utilise les services web pour lier des applications faiblement couplées ; elle se fonde sur Java pour lier des applications fortement couplées. La J2EE Connector Architecture de Sun permet de contourner le manque actuel de boîtes à outils par l'exposition directe d'interfaces sous forme de services web pour des applications écrites, par exemple, en Fortran ou en Cobol.

## Les trois couches de l'architecture des services web



Figure 1 Les trois couches de l'architecture des services web

## **La première couche de services web**

La première couche fournit un langage commun pour les services web ; ce langage permet aux applications de se connecter librement et d'échanger des informations entre elles.

Elle comprend des standards logiciels tels que :

- XML (eXtensible Markup Language) ;
- UDDI (Universal Description, Discovery and Integration) ;
- WSDL (Web Service Description Language).

Elle comprend aussi des protocoles de communications tels que :

- SOAP (Simple Object Access Protocol) ;
- HTTP (HyperText Transfer Protocol) ;
- TCP/IP (Transmission Control Protocol/Internet Protocol).

Cette première couche simplifie et rationalise l'intégration d'applications et l'échange d'informations : il n'est plus nécessaire de développer un logiciel spécifique pour faire communiquer des applications. Elle permet aux applications d'être encapsulées dans XML et de communiquer avec SOAP.

Cette première couche est actuellement la plus avancée en terme de standardisation et représente la première génération des standards de services web. Tous les fournisseurs d'infrastructure web sont, jusqu'à un certain point, alignés sur les mêmes standards pour XML, SOAP, UDDI et WSDL. Bien que ces standards ne soient pas certifiés comme normes par un organisme indépendant, ils sont néanmoins perçus comme tels par les fournisseurs d'infrastructure web. De fait, il y a un certain degré de consistance entre les différentes offres d'utilisation de ces standards.

## **La seconde couche de services web**

La deuxième couche, s'appuie sur les standards logiciels et protocoles de communication de la première couche, fournit des services communs partagés, des outils de gestion de service, de ressource et du transport. Elle permet à un utilisateur et à un fournisseur de service web de « se rencontrer » et de se connecter dans un environnement sécurisé pour effectuer des activités métier via Internet.

Parmi les standards de sécurité, on trouve :

- Kerberos pour authentifier des utilisateurs avec des jetons cryptographiques ;
- SAML (Security Assertion Markup Language) pour échanger des informations d'authentification et d'autorisation ;
- XML Signature pour spécifier comment représenter une signature dans XML ;
- XML Encryption pour définir comment chiffrer et déchiffrer un document ;
- XKMS (XML Key Management Specification)<sup>1</sup> pour spécifier comment enregistrer et distribuer des clés publiques ;
- XACML (Extensible Access Control Markup Language) pour définir les règles d'accès d'information sur un réseau.

En cours de développement par les principaux fournisseurs d'infrastructure, cette deuxième couche fait actuellement l'objet d'une standardisation prévue pour le troisième trimestre 2002<sup>2</sup>.

De nombreuses entreprises vont proposer des solutions problèmes techniques qui restent encore à régler aux dans ce domaine :

- la sécurité ;
- l'authentification ;
- l'envoi fiable de messages ;
- la gestion des sessions et des états ;
- le contrôle et la surveillance des transactions.

---

<sup>1</sup> N.D.L.R. : On pourra consulter le site du W3C : <http://www.w3.org/2001/XKMS/>

<sup>2</sup> N.D.L.R. : Pour un point exact sur l'avancement de ces travaux voir : <http://www.w3.org/>

Microsoft a introduit sa Globalk XML Web Services Architecture lors de sa conférence des développeurs professionnels en octobre 2001 à Los Angeles. Quatre spécifications de services web sont incluses : WS-Security, WS-License, WS-Router, et WS-Referral. Microsoft veut soumettre ces standards à un ou plusieurs organismes de normalisation.

### **La troisième couche de services web**

La troisième couche comprend les services applicatifs définis comme services web qui automatisent certaines tâches et activités métier. Ceci permet d'exécuter des activités métier critiques et d'effectuer des transactions via Internet. Cette troisième couche, en cours de développement, permettra d'utiliser des services web pour des activités comme le workflow, les règles métier, les transactions, la gestion de systèmes.

## **Les trois niveaux d'intégration de l'architecture des services web**

Les entreprises vont utiliser des architectures basées sur les services web pour intégrer leurs applications, leurs données et leurs processus.

IBM définit actuellement des standards pour les services web au niveau du W3C (World Wide Web Consortium) de façon à permettre l'intégration des applications, des données et des processus métier.

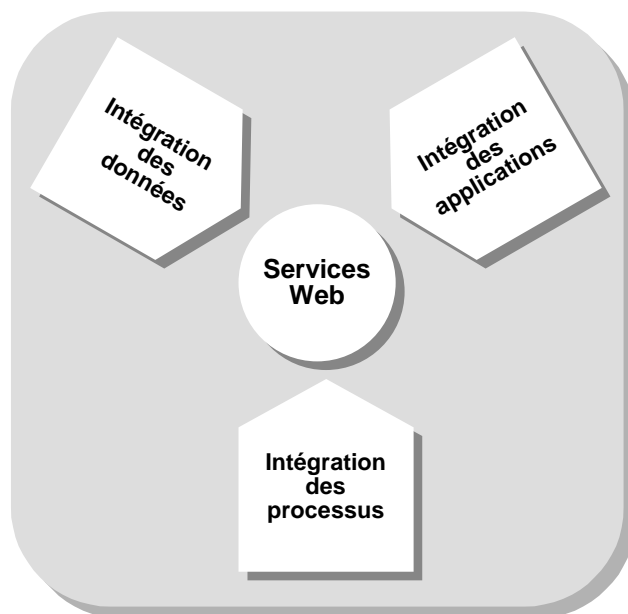


Figure 2 Les trois niveaux d'intégration des services web

### **L'intégration des applications**

Les logiciels serveurs d'IBM tels WebSphere, MQSeries Integrator, et DB2 vont inclure des fonctionnalités leur permettant une interopérabilité renforcée avec un plus grand intervalle d'intégration d'applications.

BEA va fournir une série d'adaptateurs qui permettront de se connecter à une grande variété d'applications, de bases de données et même de mainframes.

### **L'intégration des données**

XML permet de définir un langage commun pour échanger facilement des informations entre les différentes entreprises. XML fournit une grammaire commune pour donner du sens aux contenus échangés.

XML ne dispense pas de définir des standards communs d'échanges au sein des différentes industries, mais requiert que les différents participants se mettent d'accord sur le sens actuel des mots clés et résolvent au préalable les incompatibilités et ambiguïtés de sens.

Pour l'accès commun aux données, IBM développe Xperanto, une base native XML pour DB2 et WebSphere, prévue pour 2003. Xperanto permettra de manipuler les données structurées et non structurées. Xperanto utilisera XML et XQL (XML Query Language) pour permettre l'accès aux données structurées et non structurées. Xperanto intégrera les standards de services web tels que Xquery et XML Schema.

### **L'intégration des processus métier**

UDDI et WSDL donnent la possibilité aux entreprises de découvrir sur Internet des fournisseurs de services web, mais ces standards ne permettent pas encore de définir des processus et des règles métier pour orchestrer des transactions basées sur des services web sur Internet.

La prochaine étape pour les principaux fournisseurs d'infrastructure et de produits services web sera l'intégration des processus métier. Tous travaillent à l'intégration des processus métier et à leur accès commun aux données (structurées et non structurées).

Les nouvelles spécifications telles WSCL (Web Services Conversation Language), et ebXML (e-business XML) permettront une approche plus souple pour décrire les flux de processus métier.

Microsoft fournit actuellement un système d'authentification Passport et .Net My Services, un ensemble de services et d'alertes<sup>3</sup> construites sur des applications de productivité personnelle. Microsoft fournira l'intégration des processus métier au travers de BizTalk Server, l'outil qui permet l'intégration d'applications et d'informations grâce à la technologie appelée Orchestration.

Talaris, Jamcracker, et MagnetPoint sont des fournisseurs de services métier au même titre que les .Net My Services de Microsoft.

Oracle inclut les différents niveaux d'intégration dans son serveur d'application Oracle 9i. Oracle fournit déjà des fonctionnalités d'EAI (Enterprise Application Integration), de B-to-B (Business to Business) d'intégration de processus métier et des services web dans son serveur d'application Oracle 9i Application Server.

IBM incorporera CrossWorld, un outil de développement d'objets métier permettant la modélisation visuelle de processus métier, avec son serveur d'application WebSphere.

IBM, Microsoft, et le groupe de standardisation Business Process Management Initiative créent actuellement des langages fondés sur XML pour décrire les processus métier. IBM propose WSFL (Web Services Flow Language) qui deviendra un standard dans le courant de l'année 2002<sup>4</sup> et le mécanisme pour manipuler son propre logiciel d'intégration de processus métier.

## **Impact sur les technologies actuelles**

### **L'évolution des ERP**

Les ERP (Enterprise Resources Planning) évolueront vers un rôle de courtier d'informations plus granulaires en utilisant la transparence de SOAP à travers différents domaines d'entreprises et les capacités de transformation de XML pour servir ses divers clients.

Des fournisseurs tels que SAP, Tibco, Vitra alignent actuellement leurs applications en exploitant les services web pour faciliter l'intégration des processus métier. Ces fournisseurs facilitent ainsi une intégration de leurs applications avec celles des autres fournisseurs sur différentes plates-formes, de manière à permettre à leurs clients de réduire les délais et les coûts relatifs à l'extension de leurs processus métier avec leurs partenaires commerciaux.

---

<sup>3</sup>N.D.L.R. Alerte est ici employé au sens de message de notification : l'alerte peut être un message SMS.

<sup>4</sup>N.D.L.R. Pour l'avancement des travaux de normalisation, on consultera, encore et toujours le site du w3c : <http://www.w3.org/>

## **L'évolution des ASP**

Les services web vont contourner la limitation des ASP (Application Service Providers) qui demandent une forte adaptation des logiciels aux besoins des clients. Au lieu d'offrir des applications monolithiques qui doivent être adaptées au besoin du client, ils proposeront des services web de granularité plus faible.

Les ASP vont devenir des WSP (Web Service Providers). Les ASP vont migrer de leur rôle de fournisseur de logiciels vers un rôle de fournisseur de services qui seront invoqués de façon dynamique par Internet en utilisant les répertoires UDDI. Ces fournisseurs de services donneront accès à des processus spécifiques tels que la vérification de crédit, plutôt qu'à une application complète de gestion du risque.

## **L'impact sur l'EAI**

Les entreprises qui veulent exposer leur logique applicative comme des services web et remplacer leurs API (Application Programming Interfaces) propriétaires par des interfaces standard, vont rencontrer certaines difficultés. Migrer d'un VPN (Virtual Private Network) ou d'un réseau interne vers le Web élimine une couche de communication fiable et sécurisée, mais ne permet pas encore les opérations asynchrones.

L'EAI (Entreprise Application Integration) résolvait la problématique de connexion entre les applications. Avec les services web, la difficulté n'est plus de faire communiquer des systèmes disparates, mais de favoriser l'orchestration des processus métier.

Les services web, à l'inverse des technologies d'intégration précédentes, sont basés sur des standards pour exposer et connecter la logique applicative sans encourir les coûts, les délais et les efforts des approches EAI. Ils vont simplifier l'utilisation de services entre applications.

La promesse des services web d'éliminer la complexité de l'EAI est attrayante pour les responsables informatiques qui espèrent bien réduire leurs coûts informatiques avec cette nouvelle technologie.

## **Impact sur CRM**

Les applications CRM (Customer Relationship Management) sont généralement les premières impliquées par l'intégration des services web.

- D'une part, les applications CRM sont souvent les applications les plus récemment développées par les entreprises ; la migration vers des services web sera d'autant plus rapide.
- D'autre part, les applications CRM doivent accéder à des données et des transactions à partir du Web, ce qui est grandement facilité par l'utilisation de services web.

Des entreprises comme Salesforce.com, Salesnet, et Upshot concentrent actuellement leurs efforts sur la définition de services web et récoltent dès à présent les bénéfices de l'utilisation d'une architecture ouverte. Elles offrent à leurs clients une intégration facile de leurs données CRM avec des applications existantes grâce à XML ce qui simplifie grandement l'interopérabilité de leurs applications CRM.

## **Un cas concret d'utilisation de services web**

Le traitement d'une demande de crédit dans une banque est un processus complexe. Ce processus analyse des demandes de crédit et détermine la probabilité de remboursement du prêt tout en assurant la compatibilité avec les lois et réglementations contrôlant l'obtention de crédits.

La demande de crédit qui est naturellement complexe et non standardisée, demande à être traduite en prestations bancaires, avec une analyse du montage financier. En particulier, il faut satisfaire les deux contraintes suivantes :

- La réglementation limite l'accès à certains produits de crédit ;
- On doit vérifier la solvabilité de la contrepartie.

Ce processus métier comprend de nombreuses activités, dont :

- L'analyse du risque de crédit ;
- L'obtention de l'accord final ;

- La préparation des documents de prêts ;
- La signature du contrat.

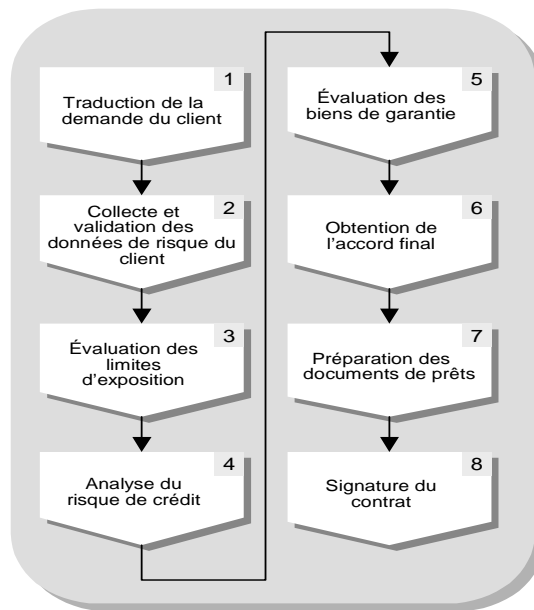


Figure 3 Processus de traitement d'une demande de crédit

Ce processus fait intervenir différents participants comme la banque, les bureaux de gestion des historiques de crédit, les institutions financières de garantie du risque de crédit, ...

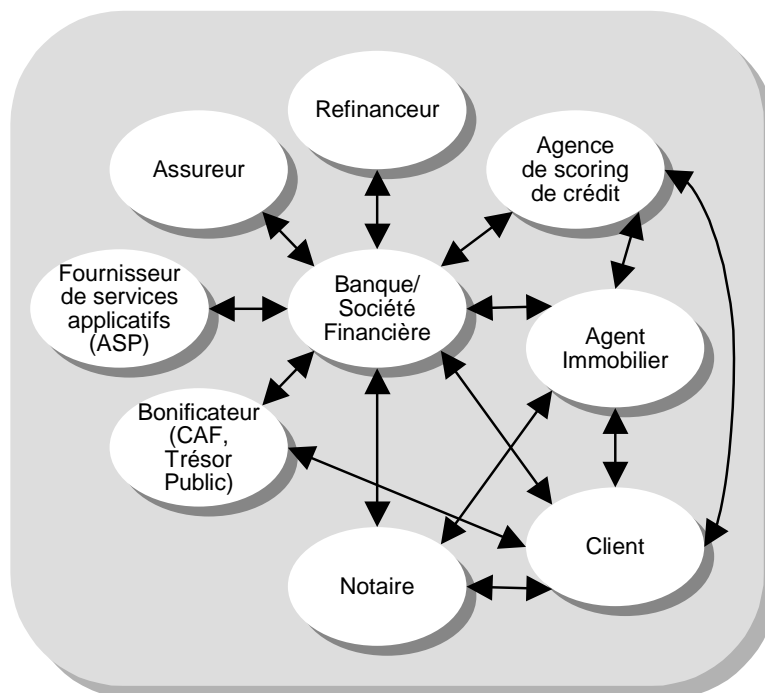


Figure 4 : Acteurs principaux d'une demande de crédit

Dans une architecture traditionnelle, la banque exécute ce processus grâce à une application monolithique complexe dont l'automatisme ne couvre souvent qu'une partie des activités. Cette application prend à sa charge certaines activités du processus et ne les exécute pas forcément de la meilleure façon. Dans le meilleur des cas, elle requiert des liaisons dédiées très chères avec les différents partenaires et fournisseurs de l'entreprise

Des interfaces applicatives complexes sont nécessaires pour maintenir la cohérence et l'interaction des différentes applications appartenant à des entreprises différentes. Les bases de données sont figées et peu intégrées.

Le processus utilise souvent des interfaces et des traitements manuels ou semi automatisés. Le processus n'est parfois que partiellement automatisé ; certains échanges avec les entreprises partenaires et fournisseurs, sont généralement exécutés manuellement au moyen de communications téléphoniques assorties de transmissions de télécopies.

En conclusion, le processus n'est ni optimisé, ni réactif. Il est sujet à des erreurs et souvent très coûteux à développer et à maintenir.

Une architecture basée sur les services web rend le processus beaucoup plus flexible, automatisé, efficace, et améliore sa qualité. Internet remplace les lignes dédiées. Un ensemble de services web remplace l'application monolithique. Certains services sont développés par l'entreprise, certains sont loués à des entreprises spécialisées et d'autres sont loués à des entreprises clientes. Au lieu de maintenir son propre système de traitement des crédits, la banque peut utiliser une approche modulaire en utilisant des services web mis à sa disposition par un ensemble de fournisseurs.

La banque peut utiliser différentes variantes d'un même processus métier pour des domaines différents. Par exemple, elle peut traiter différemment l'analyse des risques de crédit pour un prêt automobile ou pour un prêt immobilier.

En conséquence, la banque est libre de se connecter automatiquement à l'institution financière la plus compétente pour chaque activité. L'automatisation complète du processus permet un gain de temps et améliore la fiabilité des transactions. La banque peut changer facilement de fournisseurs afin d'utiliser la meilleure implémentation d'un processus. La variabilité et l'optimisation des processus métier sont ainsi assurées.

## **Les bénéfices des services web**

Compte tenu des limites actuelles des services web, de leur état de standardisation, et du développement en cours des solutions nécessaires, les services web ne produiront tous leurs bénéfices qu'à moyen et à long terme.

Le déploiement des services web permettra la réduction des coûts, l'amélioration des gains de productivité et la génération de nouvelles sources de revenus.

Les avantages compétitifs seront acquis par la rapidité de déploiement de nouvelles offres sur le marché, des fonctionnalités améliorées, et une meilleure intégration avec les acteurs périphériques de l'entreprise.

### ***Réduction de coûts et gains de productivité***

L'utilisation des services web représente une façon plus efficace de gérer le système d'information en permettant une réduction des coûts informatiques et en offrant des gains de productivité.

Les entreprises économiseront la création d'applications internes. Au lieu de développer et de maintenir des applications internes uniques, les entreprises pourront louer les fonctionnalités dont elles ont besoin, à d'autres entreprises qu'elles soient fournisseurs, partenaires ou même concurrentes.

L'acquisition de nouvelles fonctionnalités auprès d'autres entreprises leur assurera une croissance plus rapide.

La capacité « plug-and-play » standardisée des services web permettra aux entreprises d'externaliser des processus et des activités métier pour réduire les coûts ou améliorer la qualité de service.

Les entreprises pourront obtenir des gains de productivité par l'ajout et le changement incrémental de fonctionnalités. En permettant aux entreprises d'acheter seulement les fonctionnalités nécessaires, les coûts informatiques seront sensiblement réduits et la productivité accrue.

En reportant la responsabilité de développement et de maintenance de ces fonctionnalités vers des entreprises externes, les effectifs du département informatique pourront être réduits.

Les services web offrent un potentiel d'amélioration des capacités et de l'efficacité des applications existantes qu'elles soient anciennes ou plus récentes telles les ERP ou les applications CRM. Ils permettent de capitaliser des ressources applicatives existantes insuffisamment exploitées et de prolonger leur durée de vie pour préserver les précédents investissements dans le système d'information.

Les services web offrent une infrastructure à faible coût pour l'intégration d'application, qui remplace les investissements en middleware complexe coûteux à développer. Les services web ne vont pas supprimer tous les coûts et les problèmes d'intégration, mais ils offrent des opportunités de réduction des coûts et des délais requis pour atteindre l'interopérabilité des applications.

Les gains de productivité les plus importants seront obtenus aux frontières de l'entreprise avec les processus de gestion de la relation client ou de la gestion de la chaîne d'approvisionnement. La résolution de la discontinuité des processus métier entre entreprises apportera non seulement des opportunités de réduction de coûts, mais aussi de croissance.

Ceci permettra aux entreprises d'être plus réactives par rapport aux besoins du marché en adaptant leurs processus et leurs relations externes.

Les services web réduiront le risque d'utiliser des technologies en voie d'obsolescence. Les fournisseurs de services web sont tenus de fournir les dernières technologies pour être compétitifs sur le marché. Désormais, les entreprises ne seront plus liées à des applications bâties sur des technologies dépassées et maladroitement mises en œuvre.

### ***Génération de nouveaux revenus***

À plus long terme, les entreprises exploiteront les services web pour accroître leurs revenus. Elles ne se limiteront pas à utiliser des services web, mais deviendront aussi des loueurs de services web, ce qui générera de nouvelles sources de profits, potentiellement très lucratives.

La frontière entre fournisseurs et clients deviendra plus floue, chacun pouvant jouer à la fois l'un et l'autre rôle. Les entreprises achèteront des services web dans des domaines où leur compétence n'est pas assez développée, et vendront des services web dans des domaines où leur compétence est établie. Les fournisseurs de services web spécialisés deviendront des clients de leurs propres clients en intégrant certaines de leurs fonctionnalités.

Les entreprises deviendront, elles-mêmes, des fournisseurs de service web qu'elles vendront à d'autres entreprises qu'elles soient concurrentes ou spécialisées dans la location de services web. Elles offriront leurs compétences métier non critiques à des entreprises clientes. Elles mettront à disposition d'autres entreprises, sous forme de services web, certaines parties de leurs propres processus métier jugées non confidentielles, pour lesquelles elles auront développé une compétence reconnue et recherchée sur le marché.

## **Les avantages technologiques des services web**

Une architecture basée sur les services web offre des avantages indéniables par rapport aux précédents types d'architectures, en particulier l'ouverture et la modularité.

Les services web permettent d'atteindre des objectifs variés :

- l'intégration d'application à l'intérieur de l'entreprise ;
- l'ouverture sur le web d'applications existantes ;
- ainsi que l'interconnexion et l'intégration avec des partenaires, des fournisseurs et des clients.

### ***Amélioration de la flexibilité des processus métier***

L'utilisation des services web induit une plus grande variabilité et flexibilité des processus métier, dont l'encapsulation complète dans des services web permettra leur optimisation et rationalisation.

Les services web réduisent les dépendances par rapport aux systèmes d'exploitation, aux serveurs d'application et aux langages de programmation. Les processus métier peuvent s'exécuter en arrière plan sans que les utilisateurs aient à s'inquiéter des différences d'architecture et d'infrastructure.



Les services web permettent d'associer et d'apparier des parties d'applications en fonction de leurs fonctionnalités et non plus de leurs contraintes techniques. Ils encapsulent et masquent la logique applicative et les données pour faciliter la réutilisation de différentes fonctionnalités.

Inclure et offrir des fractions de logique métier à l'intérieur de services web permettront une plus grande flexibilité et une meilleure adaptation aux besoins. Les entreprises vont pouvoir redéfinir leurs systèmes d'information comme une mosaïque de services web en choisissant les plus performants et les plus adaptés à leurs compétences.

### ***Amélioration des capacités d'interconnexion***

Les services web permettent de réduire les coûts associés à la construction et à la maintenance des connexions avec des partenaires commerciaux, en fournissant une capacité de connexion peu coûteuse basée sur l'Internet. Ils donnent aux entreprises la possibilité d'appeler sur Internet des services fournis par d'autres entreprises.

Ils suppriment le besoin de créer des connexions dédiées de point à point entre différentes applications. Ces connexions interentreprises sont souvent complexes à développer, difficiles à maintenir, non flexibles et figées, et ont tendance à proliférer quand les besoins d'interconnexion entre applications se font sentir.

Les services web facilitent la communication entre systèmes disparates. Disposer de protocoles et de standards de bas niveau permet à des applications disparates de communiquer facilement. L'utilisation des mêmes standards et protocoles d'échange d'information et de transaction va accroître la flexibilité d'interconnexion entre applications.

Avec une architecture service web, les couplages entre applications s'assouplissent. Les connexions dédiées sont remplacées par la publication d'interfaces qui permettent à des applications d'interagir librement avec d'autres applications, sans avoir à programmer une connexion spécifique.

Les services web permettent de construire et d'intégrer des applications distribuées à la fois à l'intérieur des entreprises et au-delà des frontières de l'entreprise. Ils rendent plus flexible la collaboration non seulement à l'intérieur de l'entreprise, mais aussi avec des partenaires extérieurs.

### ***Amélioration des capacités d'intégration***

L'objectif des services web est de permettre aux entreprises de se connecter à des services fournis par d'autres entreprises. Cet objectif présuppose naturellement une intégration interne préalable des systèmes d'information.

L'intégration complète interentreprises de processus métier est bien plus complexe que l'intégration interne de processus métier au travers d'applications internes.

C'est à ce niveau que les limites actuelles des architectures et des processus se font le plus ressentir ; elles sont dues à l'hétérogénéité des systèmes et des architectures propriétaires et à la difficulté d'échanger des informations entre entreprises.

Les services web fournissent l'infrastructure technologique pour l'intégration des processus, des applications et des données avec celles de leurs partenaires, fournisseurs, et clients. Ils augmentent la flexibilité du partage d'information et de l'interaction entre applications.

Les entreprises vont basculer d'un modèle propriétaire à un modèle d'intégrateur de ressources existantes. Elles se focaliseront de plus en plus sur l'assemblage et la coordination de processus métier qui s'étendront au-delà des limites de l'entreprise.

Les services web vont permettre aux entreprises l'externalisation de certains processus métier fournis par une autre entreprise plus compétente. Les entreprises se procureront auprès d'autres entreprises des éléments de processus métier.

Ceci représente une opportunité pour les entreprises voulant lier leurs applications internes, échanger des données, interagir, et effectuer des transactions à l'extérieur des frontières de l'entreprise.

La localisation d'une fonctionnalité à l'intérieur ou l'extérieur de l'entreprise deviendra secondaire par rapport à la capacité de découvrir et d'intégrer ces fonctionnalités dans le système d'information.

## Les limites actuelles des services web

XML, qui existe depuis plus de 5 ans, est le plus mature des standards. En revanche, SOAP et UDDI ont cependant encore quelques problèmes à résoudre.

SOAP, bien adapté pour des transactions de type requêtes et réponses, ne permet pas encore d'exécuter des transactions complexes. SOAP ne peut diffuser des messages ou transmettre simultanément à plusieurs destinataires.

UDDI ne permet pas encore la découverte dynamique, par laquelle un utilisateur pourrait aisément localiser un service web approprié et l'utiliser à son gré.

Le déploiement des services web dépendra du niveau de sécurité des connexions entre les différents partenaires, notamment avec les nouveaux standards XML nécessaires pour sauvegarder l'intégrité des transactions au-delà des limites de l'entreprise.

Il n'y a, pour l'instant, pas encore d'accord entre les différents fournisseurs sur les spécifications et les normes de sécurité. IBM n'a pas encore soutenu publiquement la Global XML Services Web Architecture. IBM est actuellement en discussion avec Microsoft pour utiliser ces spécifications à mesure qu'elles deviennent de plus en plus matures, sous réserve qu'elles satisfassent les besoins d'IBM.

L'interopérabilité des standards entre les solutions fournies par Microsoft, Sun, IBM et BEA sera des plus importantes pour permettre de tirer pleinement avantage des services web.

L'architecture de services web n'est pas encore suffisamment robuste pour satisfaire des fortes charges de plus de 3 000 transactions par seconde.

## Les risques associés à la migration vers les services web

Les services web offrent un ensemble de règles standardisées pour coupler des applications. Mais en soi cela n'est pas suffisant pour récolter les bénéfices escomptés.

La réussite des services web viendra non seulement de l'encapsulation des applications existantes, mais surtout de leur décomposition et de l'encapsulation de leurs différentes composantes.

Utiliser des services web pour lier des systèmes disparates va demander aux entreprises de redéfinir l'architecture de leurs systèmes d'information.

Recréer des applications sur une architecture plus moderne requiert de séparer la logique des processus métier de leur présentation dans une dissection sujette à l'erreur, en particulier lorsque le code est insuffisamment documenté. Préserver la viabilité de ces investissements peut apparaître souvent plus avantageux que de se lancer dans des changements importants non exempts de risques.

Les entreprises vont devoir décomposer leurs applications en éléments de plus en plus fins et redéfinir ces éléments de façon à motiver leurs clients potentiels.

Les services web peuvent éventuellement accroître les coûts opérationnels s'ils sont mis en œuvre comme une couche supplémentaire d'interopérabilité. S'ils ne sont pas utilisés pour remplacer le middleware existant, les services web vont simplement ajouter une nouvelle couche logicielle qui augmentera la complexité des systèmes actuels, sans apporter de gains substantiels.

## Une approche recommandée de migration vers les services web

Tenter de moderniser les applications existantes est un changement porteur d'un certain niveau de risque.

Les entreprises ne sont pas tenues de changer d'un seul coup tout leur système d'information. Elles ont intérêt à entreprendre une migration progressive.

Dans un premier temps, les entreprises peuvent utiliser en interne les services web pour améliorer leur processus de développement et atteindre une meilleure intégration de leurs applications. Elles peuvent interconnecter, peu à peu, leurs applications en s'appuyant sur l'architecture ouverte et évolutive des

services web. Elles peuvent commencer par redéfinir leurs interfaces applicatives sous forme de service web sans pour autant changer leurs applications.

Dans un second temps, les entreprises utiliseront les services web à l'extérieur des frontières de l'entreprise pour obtenir une meilleure intégration au sein de leur réseau de valeur, se connecter avec des fournisseurs externes, soutenir des partenariats interentreprises. Elles peuvent s'interconnecter avec d'autres entreprises au fur et à mesure que des fournisseurs crédibles émergent sur le marché. Elles pourront décomposer leurs applications en fonctionnalités plus granulaires pour les transformer en services web pour optimiser leurs processus métier et les rendre plus flexibles sans mettre en péril leurs interconnexions internes et externes. En exposant, une à une, leurs applications de telle sorte qu'elles puissent être trouvées et accédées par d'autres applications via Internet, les entreprises vont traiter leurs besoins à court terme tout en se positionnant pour le futur.

Dans un troisième temps, les entreprises pourront rendre disponibles sur le marché certaines parties de leur processus métier pour générer des revenus supplémentaires. Elles pourront vendre sur le marché leur compétence fonctionnelle et métier pour des activités ou des processus qui ne représentent pas un avantage compétitif et qu'elles peuvent éventuellement partager avec des concurrents. Les entreprises devront peu à peu partager leurs standards avec un nombre grandissant de partenaires, de fournisseurs et de clients. Une approche incrémentale est des plus conseillée, car la collaboration au sein d'un grand groupe d'entreprises est difficile à obtenir rapidement.

## **L'impact des services web sur la gestion du système d'information**

Au début de la révolution Internet, HTTP et HTML ont changé définitivement la façon dont on publiait et utilisait des documents. Par la suite, XML a changé la façon dont les applications publiaient et utilisaient des objets métier. L'avènement des services web va initier une série de changements qui se manifesteront au cours des prochaines années.

Les services web fournissent une architecture ouverte basée sur l'Internet pour connecter des processus métier. Les services web vont introduire un nouveau style d'informatisation. Au lieu de construire des applications, les développeurs construiront des services web qui auront la capacité de s'intégrer les uns aux autres en utilisant des protocoles tels que XML, SOAP, et UDDI. Les développeurs créeront des services destinés à être assemblés ultérieurement dans diverses applications.

Des services web dimensionnés pour résoudre des problèmes métier discrets remplaceront les applications monolithiques qui couvrent un éventail très large de fonctionnalités.

Au cours des prochaines années, le recours à un important marché de fournisseurs de services web fera réaliser des économies et offrira des possibilités croissantes de collaborations entre les entreprises.

Les services web vont changer la façon dont les entreprises voient leur système d'information. Les services web vont fondamentalement modifier la manière dont les entreprises développent, déploient et gèrent leurs systèmes d'information.

Le changement le plus profond viendra de la façon dont les applications seront construites et déployées. Les services web vont encourager la création de fonctionnalités plus granulaires que celles des applications actuelles. Ils vont permettre de voir les logiciels comme des services qui pourront être sollicités et assemblés différemment en fonction des besoins métier.

Les entreprises ne feront plus de changements massifs mais progressifs de leurs systèmes d'information, réduisant les risques liés au remplacement et à la création de nouvelles applications.

Les entreprises vont pouvoir dans les prochaines années basculer d'un modèle informatique basé sur des produits à un modèle basé sur des services. Une fois l'infrastructure et les standards en place, les départements informatiques vont évoluer progressivement vers ce modèle de service. Quand les services seront capables de se découvrir dynamiquement les uns les autres, les applications et les infrastructures technologiques pourront être décomposées en composants logiques qui pourront être utilisés différemment en fonction des besoins.

Les entreprises utiliseront les services web pour externaliser des parties non critiques de leurs processus métier. La plupart des entreprises choisiront de conserver la maîtrise en interne de processus métier pour lesquels elles ont une compétence pointue qui leur procure un avantage compétitif.

Les entreprises achèteront les composants de leurs systèmes informatiques comme des services web accessibles via Internet plutôt que d'être propriétaires d'applications développées et maintenues en interne. Elles ne seront facturées que pour l'usage de services informatiques au lieu de financer en permanence la maintenance de leurs applications et de leurs centres de données.

## **L'impact des services web sur le rôle du directeur informatique**

Les problèmes d'intégration d'applications, de données et de processus métier, relèvent, au premier plan, des préoccupations des responsables informatiques.

Les directeurs informatiques auront l'opportunité d'externaliser des processus et des activités métier en achetant ou louant des services web à des fournisseurs.

Ils devront capitaliser l'expérience, la compétence et les implémentations actuelles de manière à pouvoir vendre à d'autres entreprises certaines parties de leurs applications pour en tirer des profits substantiels. Les départements informatiques ne seront, dès lors, plus perçus comme des centres de coûts, mais aussi comme des centres de profit. Les directeurs informatiques deviendront des entrepreneurs puisque leur département informatique sera devenu aussi un courtier de services vendus à d'autres entreprises.

Ils devront être capables de structurer et de gérer l'accroissement des relations et dépendances avec d'autres entreprises. Au sein de leurs industries respectives, ils devront être capables d'influencer et de négocier les standards d'échange d'informations et d'exécution de transactions.

Les directeurs informatiques vont devoir apprendre à définir des standards communs de représentation d'information et d'interface applicative entre entreprises. Habités à définir en interne ces standards, ils devront s'adapter à la prise de décisions collégiales avec des rapports non hiérarchiques, pour permettre la collaboration électronique entre les entreprises.

Les directeurs informatiques devront définir la bonne mesure entre la coopération et la compétition. Peu d'entreprises auront la force d'imposer leurs standards sur leur marché. Même si elles en sont capables, elles n'ont pas forcément intérêt à le faire dans un marché devenu de plus en plus complexe et dynamique. Développer de la confiance avec ses partenaires commerciaux tout en les influençant dans une direction favorable deviendra bien plus important que de définir de façon unilatérale des standards d'échange.

## **Conclusion**

Les services web auront un impact important sur les « business models » des entreprises, leurs offres, et leurs processus métier.

Les services web vont profondément changer la nature et la dynamique des réseaux de valeur des entreprises, en leur permettant de capitaliser des compétences métier, de louer des compétences métier auprès d'autres entreprises, et de vendre leurs compétences métier à d'autres entreprises.

Les standards des services web évolueront au fur et à mesure de l'intégration externe des processus métier des entreprises. Ils seront promus par des entreprises disposant déjà de réseaux d'échanges commerciaux, des consortiums industriels ou des fournisseurs spécialisés dans la définition de standards pour une industrie donnée.

Ainsi, les avantages induits par les services web s'épanouiront au rythme de l'ouverture des processus des entreprises aux services web et du développement de ces services par des fournisseurs spécialisés.

*Laurent Kurylo  
Senior Manager, CSC Peat Marwick,  
en stratégie et management des systèmes d'information*

## Bibliographie

Boar Bernard H., The Art of Strategic Planning for Information Technology, John Wiley & Sons, 2nd Edition, November, 10 2000, ISBN 0471376558

Boar Bernard H., Constructing Blueprints for Enterprise It Architectures, John Wiley & Sons, 1ere edition, Octobre 26 1998, ISBN 0471296201

Boar Bernard H., Practical Steps for Aligning Information Technology with Business Strategies: How to Achieve a Competitive Advantage, John Wiley & Sons 1st edition, December 3 1994, ISBN 0471076376

Cook Melissa A., Building Enterprise Information Architecture: Reengineering Information Systems, Prentice Hall PTR 1st edition, January 22 1996, ISBN 0134402561

Haag Stephen, Cummings Maeve, McCubbrey Donald J., Management & Information Systems for the Information Age, McGraw-Hill Higher Education, 3rd edition, July 27 2001, ISBN 0072458720

Hagell John III and Brown John Seely, Your Next IT Strategy, Harward Business Review, October 2001

Spewak Steven H., Hill Steven C., Enterprise Architecture Planning : Developing a Blueprint for Data, Applications and Technology, John Wiley & Sons, September 1993, ISBN: 0471599859



Square des Utilisateurs

# Vision'COM 2002

*3<sup>ème</sup> édition de l'Observatoire de la communication des entreprises des technologies de l'information*

## L'observatoire Vision'Com : 3<sup>ème</sup> édition

Vision'COM est un observatoire exclusivement dédié à la communication des entreprises évoluant dans l'univers des technologies de l'information. Cette étude a pour objectif de dresser le **panorama annuel** des canaux et outils utilisés et d'analyser les **tendances** qui se dégagent en matière de communication.

### **Exhaustif : la communication est globale**

Vision'COM couvre tous les aspects de la communication globale des entreprises :

- Le **canal direct** (de l'entreprise vers la cible) : communication institutionnelle, site Internet, marketing direct ou téléphonique, relations extérieures (salons et conférences), communication événementielle, publicité, relations partenariales, parrainage (sponsoring et mécénat) ;
- Le **canal Ressources Humaines** : recrutement et communication interne ;
- Le **canal Presse** (relations presse) : dossier, communiqué, voyage, interviews, retombées presse.

### **Unique : la communication du secteur des technologies de l'information**

L'originalité de Vision'COM est de s'adresser **exclusivement aux entreprises du secteur informatique** : éditeurs de logiciels, SSII, intégrateurs, cabinets de conseil, acteurs internet et e-business, fournisseurs d'accès, réseaux, télécoms, constructeurs, distributeurs, organismes de formation...

Contrairement à d'autres études qui s'intéressent aux grandes entreprises françaises, Vision'COM analyse la communication d'entreprises de toutes tailles : de 20 à plusieurs milliers de collaborateurs.

### **Panel 2002**

L'observatoire Vision'COM 2002 a été adressé à un **panel de 2.143 entreprises** représentatives du secteur informatique, dont **691 SSII** et intégrateurs, **687 éditeurs** de logiciels, **260 cabinets** de conseil. Le **taux de réponses s'est élevé à 5,1%**.

Les éditeurs de logiciels ont répondu à 8,2% (6,9% en 2001), viennent ensuite les SSII avec un taux de réponses de 5,5% (3,1% en 2001) et enfin les cabinets de conseil avec 5,4% (3,5% en 2001).

Ces taux de réponses en hausse révèlent une **professionnalisation** de l'activité « communication » au sein des entreprises du secteur des technologies de l'information et un **besoin grandissant de se situer** par rapport aux pratiques globales de la concurrence : d'où l'intérêt exprimé pour Vision'COM.

## Vision'COM 2002 sous l'angle budgétaire

### **Légère baisse du budget alloué à la communication**

En moyenne, les entreprises dédiées aux technologies de l'information dépensent **3,3% de leur chiffre d'affaires** pour leur communication (contre 3,5% en 2001 et 3,0% en 2000).

Bien que les éditeurs de logiciels aient réduit leur budget de 1,5% par rapport à l'année dernière, ils **arrivent toujours en tête en terme d'investissement** et consacrent 4,7% de leur chiffre d'affaires à leur communication en 2002, contre 6,2% en 2001.

En deuxième position, les sociétés de services informatiques consacrent 2,2% de leur chiffre d'affaires en 2002 : ce ratio est en **hausse de 0,8% par rapport à 2001**.

Enfin, les cabinets de conseil consacrent 1,2% de leur chiffre d'affaires en 2002 : ce ratio est en **baisse de 2,4% par rapport à 2001**.

Par ailleurs, **plus l'entreprise est grande, plus le ratio « budget Com./CA » est petit**. Les entreprises dont l'effectif est inférieur à 100 personnes consacrent à leur communication 3,8% de leur chiffre d'affaires ; 2,8% pour les entreprises de 100 à 500 collaborateurs ; 1,2% pour un effectif supérieur à 500.

- Dans les petites entreprises, inférieures à 100 personnes, le ratio a **diminué**.
- Dans les entreprises de 100 à 500 personnes, le ratio a **augmenté**.
- Dans les entreprises supérieures à 500 personnes, le ratio est **inchangé**.

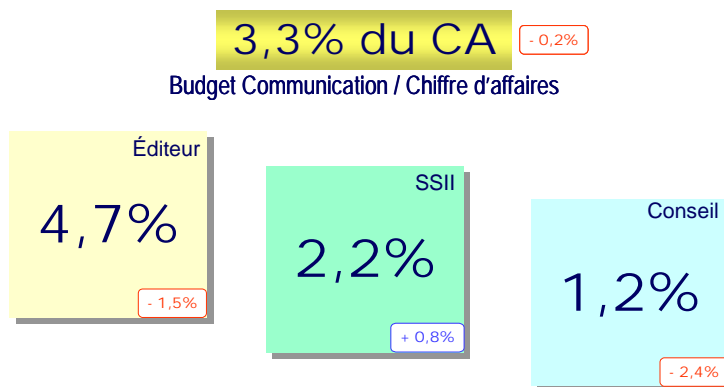


Figure 1 : Pourcentage du CA dédié à la communication par type d'activités en 2002

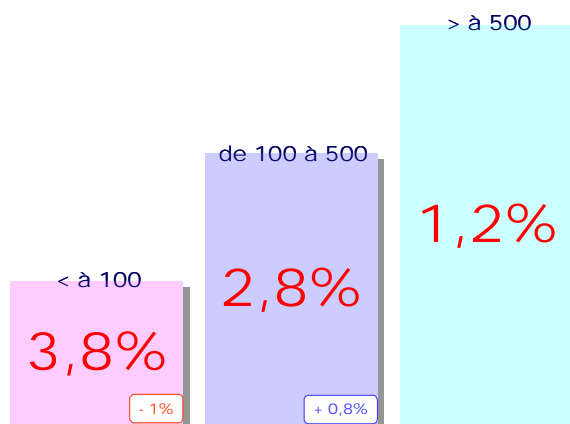


Figure 2 : Pourcentage du CA dédié à la communication par taille d'entreprises en 2002

### Nouvelle répartition budgétaire

La répartition budgétaire globale montre une **hausse** sur les canaux « **direct** » et « **Presse** » et une **baisse sur le canal Ressources Humaines**.

Les canaux « direct » et « Presse » évoluent en fonction de la conjoncture économique, à la hausse comme à la baisse selon les années. Le **canal Presse est en constante augmentation depuis 2000**.

	En 2000	En 2001	En 2002
Canal direct	77%	71%	76%
Canal Ressources Humaines	14%	18%	10%
Canal Presse	9%	11%	14%

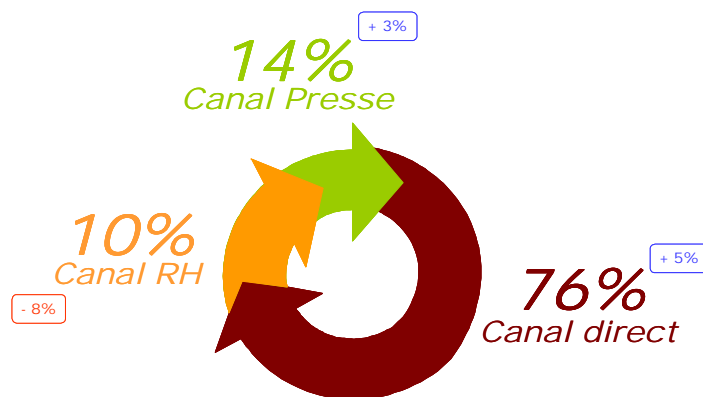


Figure 3 : Répartition budgétaire en 2002

D'un point de vue sectoriel, on note des pratiques différentes quant à l'affectation des ressources financières.

- Les **éditeurs de logiciels** augmentent leur budget dédié aux relations Presse.
- Les **SSII** baissent de 11% leur budget sur le canal Ressources Humaines.
- Les **cabinets de conseil** augmentent les canaux directs et Ressources Humaines et reviennent à un ratio plus normal pour les relations Presse : 8% en 2002 contre 20% en 2001.

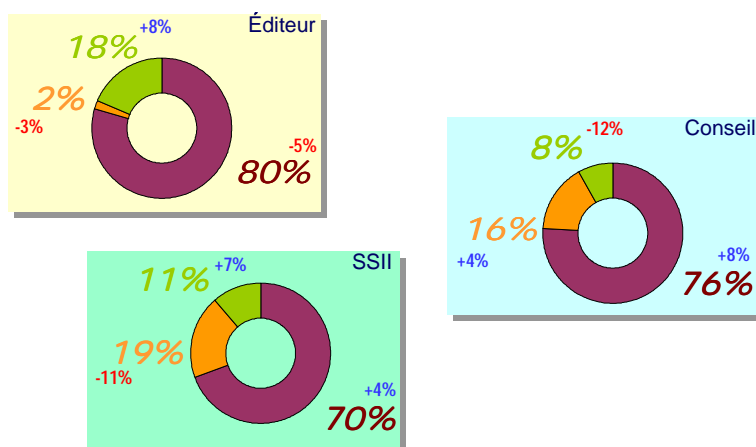


Figure 4 : Répartition budgétaire par type d'activités en 2002

## Les points-clés en 2002

### **Forte hausse du marketing téléphonique : +9%**

Outil relationnel et de proximité, le **télémarketing enregistre une hausse de 9%** par rapport à l'année dernière en ce qui concerne son utilisation par l'équipe interne : **73% des entreprises le pratiquent en 2002**, contre 64% en 2001 et 63% en 2000.

86% des éditeurs de logiciels ont recours au marketing téléphonique en interne, 71% des SSII et 57% des cabinets de conseil.

Plus la société est grande, plus elle pratique le télémarketing :

- 70% des entreprises inférieures à 100 personnes ;
- 76% de celles qui comptent entre 100 et 500 personnes ;
- 80% des entreprises de plus de 500 personnes.



### **Recrutement : recours aux cabinets de chasseurs de têtes en hausse continue**

Elles étaient **35%** en 2000, puis **42%** en 2001... et enfin **45%** en 2002 à travailler avec des cabinets de chasseurs de têtes. Cet appel à des professionnels du recrutement s'explique par la complexité des métiers et le besoin de recruter les meilleurs potentiels.

Par ailleurs, les entreprises réalisent **moins de petites annonces** : 43% en 2002 contre 48% en 2001.

Enfin, et c'est le point le plus regrettable, de moins en moins d'entreprises disposent d'un **plan dédié à la communication recrutement** : en 2002, **seulement 12%** des entreprises organisent leurs recrutements, les autres fonctionnant au coup par coup. Elles étaient 27% en 2001 et 32% en 2000 !

### **Retournement de situation pour le site Internet**

En 2001, 100% des SSII dédiaient en priorité leur site aux candidats.

En 2002, la conjoncture économique et la baisse de pression sur le recrutement placent **le client au cœur du site Internet des entreprises**.

60% des entreprises dédient leur site à leurs clients (+5% par rapport à 2001) et 55% d'entre elles le dédient à leurs prospects.

Les partenaires enregistrent aussi une hausse de 7% et les sites leur sont dédiés pour 38% des sociétés.

Les **candidats** ne sont plus au cœur d'Internet : le site leur est dédié par 42% des sociétés (**- 17% par rapport à 2001**).

### **L'outil « conférence hors salon » subit une baisse de 10%**

Il s'agit ici d'aborder des sujets de réflexion à forte valeur ajoutée. On peut aussi parler de conférences non commerciales. Il est clair que cet outil nécessite une préparation importante : proposition de sujets (acceptés ou refusés), résumés bilingues en deux formats (version courte et version longue), communication externe (clients, prospects, presse, partenaires...), préparation des transparents, répétitions, communication interne, etc.

Est-ce suffisant pour expliquer cette baisse ? En 2002, les entreprises semblent plus concentrées sur les opérations dont le retour sur investissement sera obtenu à court terme, plutôt que sur un travail d'image conçu dans la durée.

## Les faiblesses en 2002... déjà identifiées en 2001

### Des relations presse toujours peu performantes

94% des entreprises pratiquent les relations presse. Or, malgré le **recours à une agence spécialisée dans 50%** des cas (55% en 2001 et 46% en 2000), les résultats enregistrés par les relations presse demeurent faibles. **Seulement 32%** des entreprises obtiennent **plus de 50 retombées presse** (11% seulement pour plus de 200 par an).

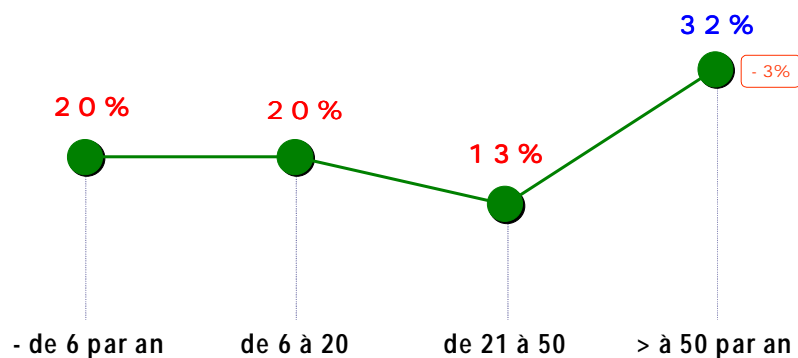


Figure 5 : Répartition globale des retombées presse en 2002

Cette année encore, les SSII ont de meilleures performances que les éditeurs de logiciels, à quasi-égalité avec les cabinets de conseil :

- 39% de SSII obtiennent plus de 50 retombées presse par an ;
- 30% pour les éditeurs ;
- 29% pour les cabinets de conseil.

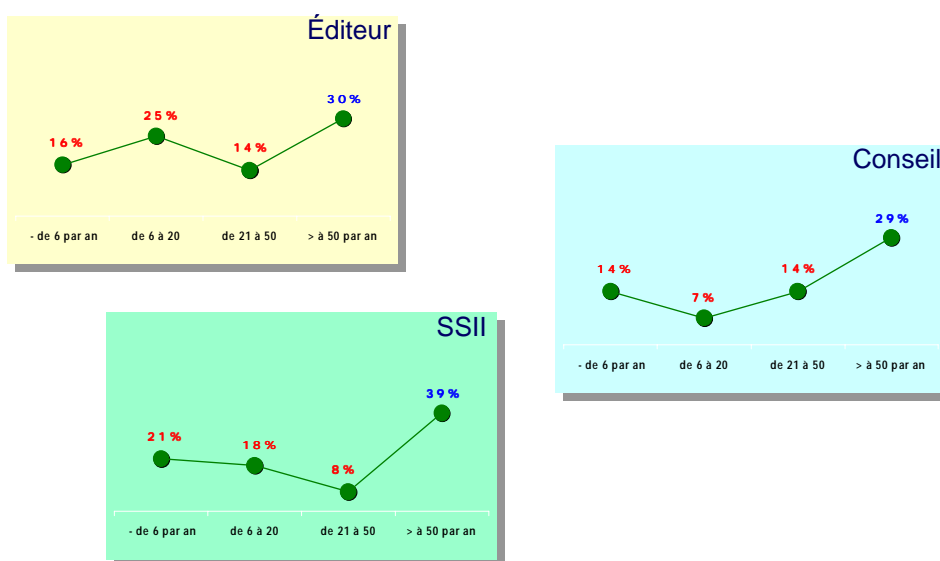


Figure 6 : Les retombées presse par type d'activités en 2002

## Des investissements publicitaires toujours épisodiques

Comme en 2000 et en 2001, les entreprises n'ont pas recours à la publicité de façon régulière, ce qui nuit à l'efficacité de l'outil.

Malgré tout, on constate une amélioration au fil des ans :

- En 2002, 54% des entreprises font de la publicité de façon épisodique.
- En 2001, elles étaient 59%.
- En 2000, elles étaient 64%.

## Encore peu d'efforts en communication interne

Comme les années précédentes, les informations diffusées en interne sont basiques : annonces des nouveaux contrats, annonces de l'arrivée de nouveaux collaborateurs, annonces des actions de communication, stratégie de l'entreprise, retombées presse, présentation des offres futures...

Peu d'entreprises diffusent des informations à valeur ajoutée et plus enrichissantes pour leurs salariés : état de l'art du marché, de la concurrence, piges de presse, résumés d'ouvrages...

## Les internautes sont toujours mal traités

D'une façon globale, les demandes d'informations qui parviennent à l'entreprise par Internet ne sont pas traitées en toute priorité : 28% des entreprises les traitent dans la semaine, 27% le lendemain, **seulement 43% les traitent immédiatement**. À noter que 2% des entreprises ne répondent pas à la question...

D'un point de vue de l'activité, les cabinets de conseil sont les moins réactifs.

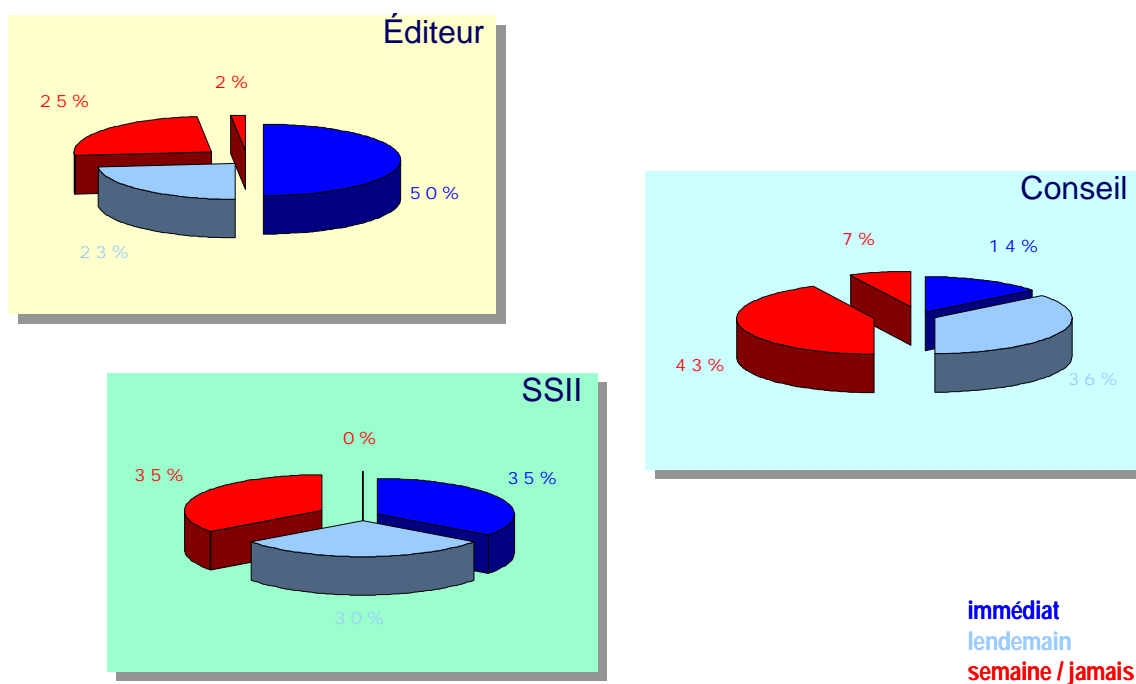


Figure 7: Le traitement des demandes sur Internet par type d'activités en 2002

La vision par taille d'entreprises révèle que les plus petites sont les plus réactives vis-à-vis des internautes... Peut-être ne subissent-elles pas le poids des procédures ?...

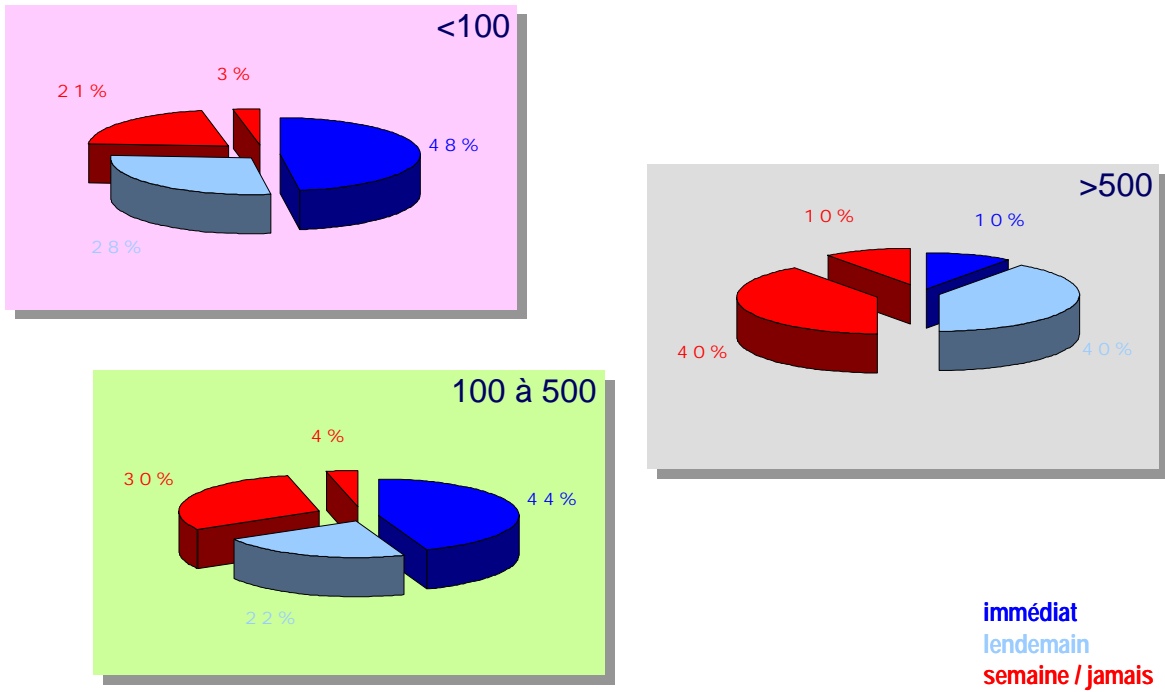


Figure 8: Le traitement des demandes sur Internet par taille d'entreprises en 2002

### Peu de mesures du retour sur investissement (R.O.I.)

Les entreprises ne pratiquent pas systématiquement l'analyse de leurs opérations de marketing : 5% des entreprises ne les analysent jamais, 37% les analysent parfois, et seulement 58% les analysent systématiquement.

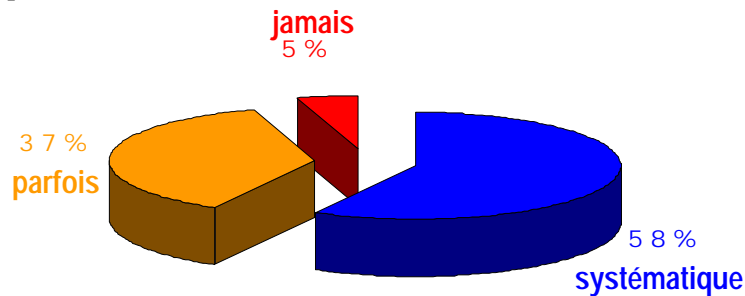


Figure 9: Marketing : la mesure du R.O.I. en 2002

La mesure de la qualité des retombées presse s'exprime ci-dessous :

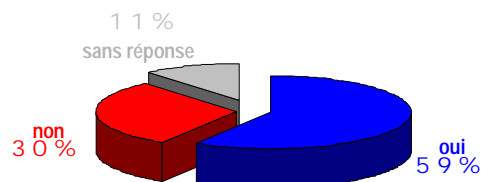


Figure 10: Mesure de la qualité

## Vision globale de la communication en 2002

À partir des grands thèmes abordés dans l'enquête, des critères sont sélectionnés sur chacun des canaux de communication. Chaque critère subit ensuite une pondération selon l'importance du rôle joué par l'outil analysé.

Par exemple :

- Sur le **canal direct**, au sujet d'**Internet**, la réponse sur le traitement des demandes des internautes est pondérée par 4 si la réponse est immédiate, par 3 si elle a lieu le lendemain, par 0 si elle intervient dans la semaine.
- Au chapitre de la **communication interne**, dans la liste des informations diffusées aux collaborateurs, celles qui ont les plus fortes pondérations sont celles à valeur ajoutée comme les résumés d'ouvrages (\*4), les pîges de presse (\*3), les analyses de la concurrence (\*3), les analyses de marché (\*3), les récits de projets (\*3). Les autres informations diffusées ne sont pas pondérées (\*1).
- En ce qui concerne les **relations presse**, l'indicateur principal est le nombre annuel de retombées presse. Ce chiffre subit les pondérations dégressives suivantes : plus de 200 retombées annuelles (\*6), de 51 à 200 retombées (\*4), de 6 à 50 retombées (\*1), et pour moins de 6 retombées par an, il est multiplié par 0.

La somme des points obtenus par chaque entreprise conduit à l'obtention d'une note sur 20. Les graphiques de la page suivante ont été construits selon cette méthode.

Entre 2001 et 2002, on note un resserrement global des notes :

- Concernant les **outils institutionnels** (plaquette société, carte de vœux, journal d'entreprise, témoignage des clients, CD-Rom, rapport annuel...), la majorité des entreprises en est dotée aujourd'hui. Cela ne constitue plus un élément différenciant, mais incontournable. Les cabinets de conseil sont légèrement en retrait par rapport aux éditeurs de logiciels et aux SSII.
- Pour **Internet**, la moyenne globale est de 10/20. Les éditeurs ont 10,5, les SSII obtiennent 10 et enfin les cabinets de conseil 8,5. La faiblesse de la note est essentiellement due au mauvais traitement des demandes des internautes et au peu de contenu à valeur ajoutée.
- La rubrique **Marketing** enregistre aussi une note moyenne de 10 par manque d'analyse en amont, une gestion de contacts peu poussée et une relation client négligée.
- Les **événements** et les relations avec les **partenaires** sont menés de façon assez homogène par les éditeurs et les SSII, les cabinets de conseil restant en retrait.
- La **publicité** obtient une note faible quelle que soit l'activité : 9/20 pour les éditeurs, 8/20 pour les SSII et 7/20 pour les cabinets de conseil. En effet, la publicité est épisodique, comme en 2000 et en 2001.
- Le **sponsoring** est plutôt pratiqué par les SSII, sans doute en soutien des opérations sur le canal Ressources Humaines (recrutement et interne).
- Le **recrutement** obtient à peu près les mêmes notes quelle que soit l'activité, alors que les SSII se distinguent en **communication interne**.
- Les **relations presse** obtiennent une note globale très faible : 9/20.

## Positionnement des entreprises sur chacun des axes de communication

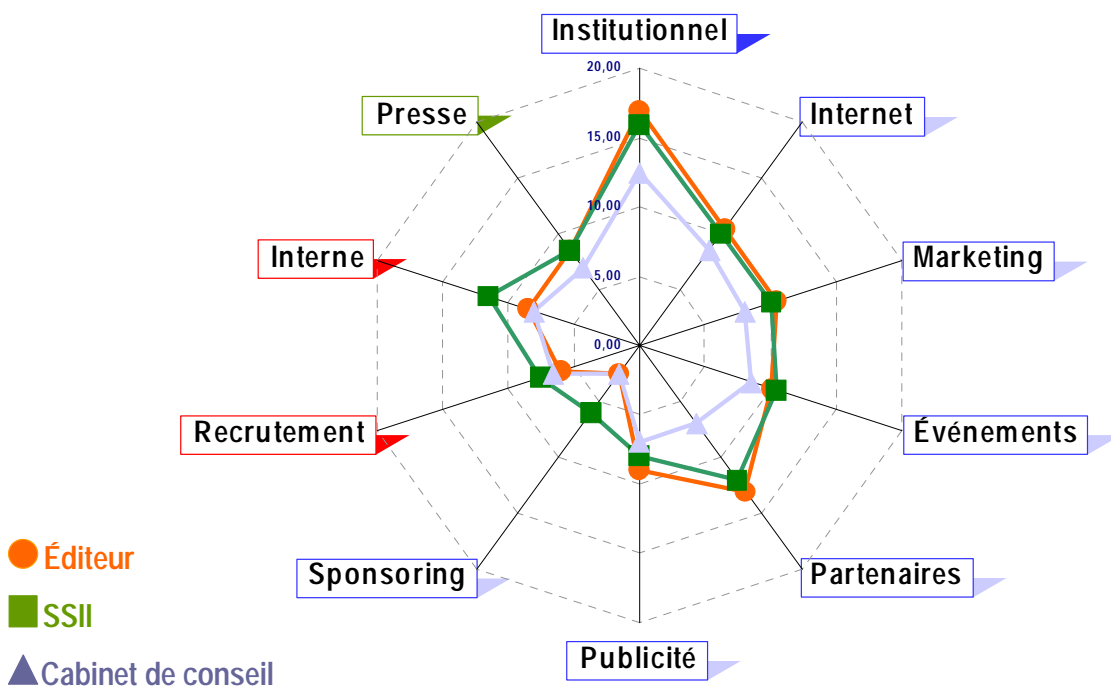


Figure 11 : Positionnement des entreprises selon leur activité en 2002

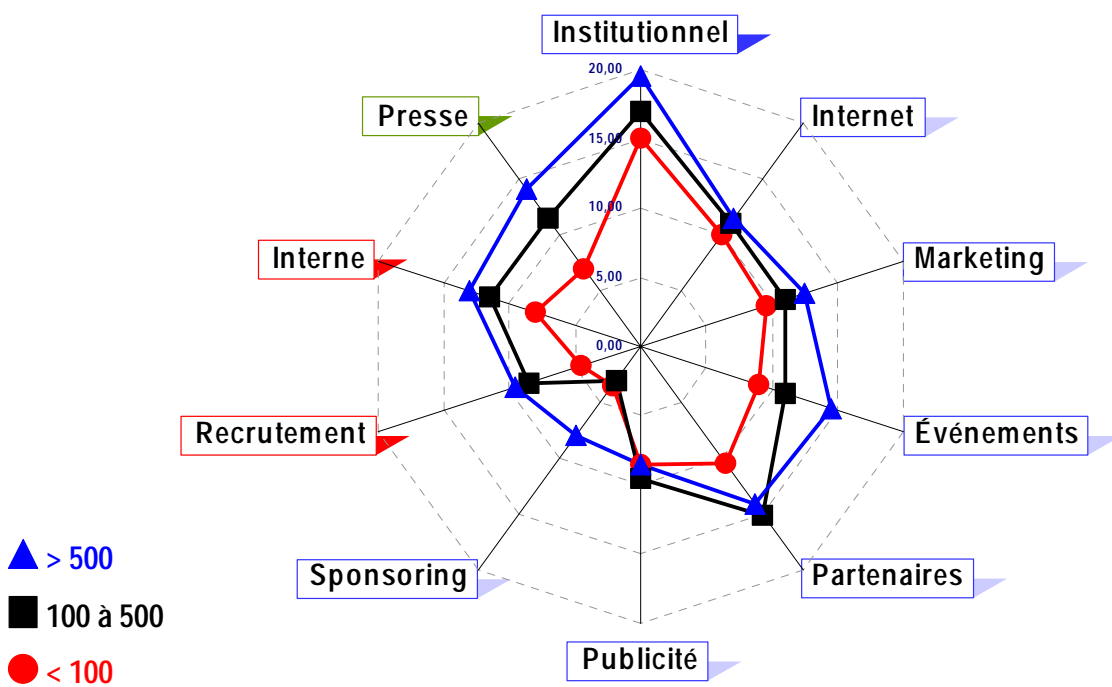


Figure 12 : Positionnement des entreprises selon leur taille en 2002

### **À quoi sert la communication d'entreprise ?**

La communication est l'ensemble des **méthodes, moyens et actions** dont dispose une entreprise pour atteindre son **public, externe et interne**.

La communication a pour objectif global de faire **connaître, comprendre et aimer l'entreprise**. Une politique de communication active doit donner confiance et rassurer la cible.

Qu'il s'agisse de gagner de la **notoriété**, d'améliorer son **image**, de diffuser de l'**information**, d'accroître ses **parts de marché**, de garder le **contact avec ses clients**... **toutes les actions de communication contribuent à la réussite et au développement** de l'entreprise.

L'image d'une entreprise est la **somme de ses différentes images** : institutionnelle, interne, financière, presse... On comprend alors aisément qu'elle n'est **ni unique, ni définitive**. Elle évolue dans le temps et peut varier selon les publics ciblés. **Une image d'entreprise s'acquiert dans la durée et se travaille de façon quotidienne**.

Aujourd'hui, toutes les entreprises ont conscience que la communication est une **activité stratégique, indispensable pour leur développement**.

### **Quels canaux véhiculent l'image de l'entreprise ?**

Pour atteindre son marché, l'entreprise utilise trois canaux différents : le canal direct, le canal des ressources humaines et le canal de la presse. Grâce à un **travail continu et simultané sur ces trois canaux**, l'entreprise parvient à se bâtir une image solide.

Le recours à l'un des canaux a une incidence notable sur les deux autres : des actions de communication sur le canal direct donne de la matière aux relations presse. Des retombées presse fructueuses apportent de la crédibilité au discours externe et de la fierté en interne. Une bonne communication RH forge une réelle culture d'entreprise. Les collaborateurs deviennent alors des relais efficaces vers l'extérieur, etc. **Les trois canaux interagissent** entre eux... et leur parfaite synergie permet de **construire une image cohérente**.

#### **Le canal direct**

Il s'adresse directement à la cible : clients, prospects, partenaires... Les outils mis en œuvre par ce canal sont des supports d'image (papier, électronique, objets, locaux...), des relations extérieures (salons, conférences...), de la publicité, du marketing, etc.

**Les messages émis en communication externe sont complètement maîtrisés**. Ils sont restitués auprès des cibles tels qu'à leur émission, ce qui ne signifie pas qu'ils sont perçus tels que lus, entendus ou vus.

#### **Le canal Ressources Humaines**

Il convient tout d'abord de distinguer les deux facettes de cette activité tournée vers les collaborateurs, selon qu'ils sont candidats pour entrer dans l'entreprise, ou qu'ils en sont déjà salariés. Dans un cas on parle de communication **recrutement**, dans l'autre de communication **interne**. La **communication RH** est la meilleure expression pour englober les deux activités qui contribuent à **féderer les collaborateurs, futurs, actuels... et passés**. En effet, une bonne communication RH permettra aux partants de conserver une bonne image de l'entreprise qu'ils quittent.

Parmi les outils utilisés, on trouve : le livret d'accueil, le journal interne, le site Intranet, la formation, les séminaires de travail, de motivation, de récompenses... les animations, les jeux et concours, etc. et, bien sûr, toute la communication, dans son sens le plus global : externe, presse, **management**... Ce dernier aspect n'est pas toujours vécu comme de la communication, cependant son rôle est déterminant par rapport aux autres supports : le plus beau livret d'accueil n'effacera jamais des tensions internes, ni une hiérarchie absente.

**Le message véhiculé est globalement maîtrisé, mais les collaborateurs se l'approprient et le diffusent à leur façon.** Plus la communication RH est intense, plus le message est retransmis et plus les collaborateurs peuvent devenir des relais efficaces : ils sont motivés, ils participent au développement de l'entreprise, ils jouent un rôle actif dans le processus de recrutement...

### **Le canal Presse**

Le paramètre fondamental concernant les relations presse est qu'il s'agit d'un **canal non maîtrisé par l'entreprise communicante**. En effet les objectifs de l'entreprise et ceux des journalistes sont différents : **l'entreprise communique, les journalistes informent**. Le moment qu'ils choisiront pour transmettre l'information, s'ils la jugent pertinente pour leurs lecteurs, n'est pas forcément celui qui convient le mieux à l'entreprise. En se lançant dans les relations presse, l'entreprise doit en être consciente et se plier à cette règle. Ce canal dispose d'un **atout incontestable par la crédibilité qu'il procure à l'entreprise**.

*Geneviève Coullault*  
*A POSTERIORI – 15 avenue Charles de Gaulle – 92100 Boulogne*  
*gcoullault@a-posteriori.com*  
*01 46 04 96 99*





# L'évolution des normes de sécurité...

**...vers plus d'auditabilité des systèmes d'information**

*Cet article présente les principales caractéristiques des aspects passés, présents et futurs de l'activité de normalisation et standardisation en matière de Sécurité des Systèmes d'Information de Santé.*

*Après un indispensable historique des diverses définitions de « sécurité » (I.T. security, sécurité des systèmes d'information et sécurité des systèmes d'information de santé), nous aborderons la distinction entre la standardisation « de facto » du passé et celle « de jure » du présent et du futur. Nous insisterons sur les aspects primordiaux des activités de la sécurité des systèmes d'information de santé, fondés sur le fait que ces systèmes exigent des normes et standards de sécurité particuliers. Pour être pertinent il est nécessaire de faire une distinction entre sécurité et qualité, entre sécurité-‘security’ et sécurité-‘safety’, entre sécurité et intimité, entre confidentialité-discrétion et confidentialité-séclusion (anonymisation ou pseudonymisation) et enfin entre auditabilité et ‘accountability’.*

*En conclusion, nous rappellerons que la normalisation n'est pas seulement une affaire d'experts mais aussi et, en priorité, le résultat des exigences des acteurs du secteur. Nous montrerons que l'auditabilité est la propriété d'avenir des systèmes d'information de santé (médicaux et hospitaliers) pour accroître la confiance à placer dans la sécurité de ces systèmes pour une meilleure qualité des systèmes eux-mêmes.*

## Préambule (introduction)

### Le contexte

Le colloque « Présent et avenir des Systèmes d'Information et Communication Hospitaliers (SICH) » organisé à l'Hôpital Européen Georges Pompidou (HEGP) aborde différents angles de vue notamment celui, transversal, de la sécurité des communications (cf. Session V : communication et sécurité).

Dans le cadre plus général de la sécurité, cet article traite de la sécurité des informations et des communications dans le contexte spécifique de la sphère santé, et dans l'environnement de l'informatique hospitalière. Il se focalise sur le « présent et l'avenir de la normalisation en informatique de santé ».

Notre propos n'est pas de passer en revue l'ensemble des normes en vigueur, en cours d'élaboration, ou en projet, dans le domaine de la sécurité des systèmes d'information de santé. Un long article ne suffirait pas à commenter les aspects conceptuels et techniques d'une seule de ces normes.

Pour une bonne compréhensibilité et ainsi une meilleure appropriation des informations, en particulier par un lecteur néophyte, nous nous limiterons (ce qui résume malgré tout quelques années.hommes d'activité en normalisation) à :

- un bref rappel des documents normatifs de référence en sécurité de manière générale : ISO 7498-2 [1], TCSEC [2], ITSEC [3], Common Criteria [4], ISO 17799 [5], GMITS 1-5 [6], ISO 10181 1-7 [7] ;
- un rapide survol des normes de sécurité tant génériques que sectorielles : ENV 12251 :2000 [8], ENV 13729 :1999 [9], ISO 17090 [10], CR 13694 :2000 [11] ;
- un parcours plus détaillé des principales normes de sécurité dédiées à la sphère santé : ENV 12924 [12], ENV 13606-3 [13], ENV 13608-1 [14], FD S 97-560 [15].

Les normes ou documents normatifs relatifs à la sécurité dans la santé, commentés plus en détail dans cet article, sont issus de trois groupes et niveaux de normalisation auxquels la France participe activement :

- national : le groupe GE-SSIS<sup>1</sup> au sein de la CNIS<sup>2</sup> d'AFNOR<sup>3</sup> ;
- européen : le groupe WG III<sup>4</sup> au sein du TC251<sup>5</sup> du CEN<sup>6</sup> ;
- mondial : les groupes WG 4 et WG 5<sup>7</sup> au sein du TC215<sup>8</sup> de l'ISO<sup>9</sup>.

### **Présentation de l'article**

Cet article se propose de faire découvrir au lecteur non initié, l'existence des nombreux travaux de normalisation effectués ou projetés en informatique de santé. Cet article montre l'ampleur et la nécessité de poursuivre ceux qui la sécurité de ces systèmes d'information de santé ; ces travaux sont complémentaires de ceux menés autour de la sécurité des systèmes d'information en globalité.

Notre exposé, en parcourant les normes les plus représentatives de l'évolution de la sécurité informatique, présentera :

- la progression de la perception de la sécurité depuis la sécurité originelle des systèmes d'exploitation, en passant par la sécurité classique des systèmes informatiques, jusqu'à la sécurité actuelle des systèmes d'information du secteur santé, voire hospitalier ;
- l'apparition des tendances actuelles et futures en matière de besoins de sécurité, plus particulièrement spécifiques à la sphère santé/social et au secteur l'hospitalier ;
- l'orientation des futures architectures de sécurité à construire pour prendre en compte ces nouveaux besoins et répondre aux questions liées aux développements des nouvelles technologies de l'information et de la communication.

La composition de cet article est la suivante :

- un historique de la définition de la sécurité (matériel) ;
- les relations entre la sécurité et la normalisation (méthode) ;
- l'évolution dans la prise en compte de normes (résultat) ;
- les tendances actuelles et à venir en sécurité (discussion) ;
- les enseignements pour la sécurité de demain (conclusion).

## **Histoires de la sécurité (matériel)**

Ce chapitre est un préalable nécessaire à une meilleure compréhension de l'évolution de la notion de sécurité – informatique à l'origine et désormais appelée des systèmes d'information – c'est-à-dire de la progression de la perception qu'ont de la sécurité les différents acteurs des systèmes d'information.

Nous verrons que la sécurité, toujours destinée à éviter les malveillances, a progressivement étendu son champ d'investigations et son spectre de besoins, depuis le strict contrôle d'accès de bas niveau, jusqu'aux garanties juridiques de bon fonctionnement.

---

<sup>1</sup> GE-SSIS : Groupe d'Experts en « Sécurité des Systèmes d'Information de Santé » de la CNIS.

<sup>2</sup> CNIS : Commission de Normalisation "Informations de Santé" d'AFNOR.

<sup>3</sup> AFNOR : Association Française de Normalisation.

<sup>4</sup> WG-III : Working Group on "Security, Safety and Quality" du TC251.

<sup>5</sup> TC251 : Technical Committee on "Health Informatics" du CEN.

<sup>6</sup> CEN : Comité Européen de Normalisation.

<sup>7</sup> WG 4 et 5 : Working Group 4 on "Security" et Working Group 5 on "Health Cards" du TC215.

<sup>8</sup> TC215 : Technical Committee on "Health Informatics" de l'ISO.

<sup>9</sup> ISO : Organisation Internationale de Standardisation.

## **Sécurité informatique**

La « sécurité informatique » dont on peut fixer l'émergence lors des années 70, est issue de travaux menés autour de la protection des systèmes d'exploitation.

Les systèmes « Multics » (cf. les anneaux) et « Unix » (droits d'accès), gèrent les conditions d'accès aux ressources de la machine et les droits d'accès aux fichiers (cf. « rwe » - read write execute). Ce sont les principales mesures de sécurité dites « logiques ».

Ces standards de facto (qui ne sont pas encore des normes de jure) utilisés par les principaux constructeurs d'ordinateurs, ont marqué cette première période.

On peut caractériser cette ère de la sécurité informatique par la notion de politiques de contrôle des droits d'accès : ainsi, se sont développées les deux premières catégories de politiques de contrôle :

- « par mandat » ou « obligatoires » (cf. 'MAC: Mandatory Access Control') ;
- « discrétionnaires » (cf. 'DAC: Discretionary Access Control').

## **Sécurité des technologies de l'information**

La « sécurité des technologies de l'information », terme apparu lors des années 80, correspond à la prise en compte d'un ensemble plus large de contraintes, de problèmes, de risques et de solutions, pour développer la sécurité des technologies de l'information, ou « I.T. Security: Information Technology Security ». ISO 7498-2 [1] première norme internationale, calquée sur le modèle ISO/OSI est fondatrice de la sécurité ; lui ont succédé une série de documents, à caractère normatif, élaborés depuis les années 80 pour permettre d'évaluer la sécurité des systèmes :

- d'abord les TCSEC – Trusted Computer Security Evaluation Criteria (Orange Book) –édités aux États Unis et apparus comme les fondements de l'évaluation de la sécurité, surtout des systèmes d'exploitation (cf. [2]) ;
- puis les ITSEC – Information Technology Security Evaluation Criteria – édictés en Europe et concurrents plus pertinents pour l'évaluation de la sécurité des systèmes (cf. [3]) ;
- et enfin, après une transition par des critères fédéraux américains (Federal Criteria), les Common Criteria – Security Techniques Evaluation for I.T. Security – édictés de part et d'autre de l'Atlantique pour fournir une norme mondiale d'évaluation de la sécurité, la norme ISO 15408 (cf. [4]).

La sécurité est, alors, considérée comme un facteur de qualité des systèmes ; c'est un argument de qualité de service, notamment pour les communications, et aussi l'un des attributs perceptifs du concept de sûreté de fonctionnement. Sa définition se stabilise autour de trois propriétés fondamentales applicables tant aux informations manipulées par les systèmes qu'aux systèmes eux-mêmes à travers leurs services, programmes, protocoles et mécanismes ; il s'agit du DIC regroupant :

- la disponibilité : les informations sont rendues disponibles selon des autorisations définies par la politique de sécurité du système ;
- l'intégrité : les informations ne peuvent être modifiées que d'une façon explicitement autorisée par la politique de sécurité définie pour le système ;
- la confidentialité : les informations ne sont pas divulguées en dehors des autorisations formellement accordées par la politique de sécurité définie pour le système.

On peut résumer cette ère de la sécurité des technologies de l'information par les concepts de politique de disponibilité – intégrité - confidentialité et de politique d'évaluation - certification de la sécurité.

## **Sécurité des systèmes d'information**

La notion de « sécurité des systèmes d'information » (proche de la définition précédente) est apparue lors des années 90, dans le souci de prendre en compte d'autres aspects que ceux strictement liés à la technologie de l'information. Ces aspects incluent la gestion de l'ensemble des facteurs qui contribuent à la mise en place de politiques de sécurité et les responsabilités qu'elles impliquent.

Les normes suivantes illustrent cette préoccupation de sécurité globale du système considéré :

- la norme ISO 17799 (issue de la British Standard 7799) désormais référence mondiale en matière de sécurité des systèmes d'information, au plan générique (cf. [5]) ;
- la série de normes ISO 13335, les GMITS, série de directives pour la gestion et l'administration de la sécurité (cf. [6]) ;
- la série de normes ISO/IEC 10181, cadre de l'ensemble des aspects de la sécurité concernant l'interconnexion de systèmes ouverts (cf. [7]).

La prise en compte des notions de responsabilité relative à la sécurité et les besoins d'auditabilité de systèmes et de leurs sécurités sont déjà présents de manière générique. Cependant, ils ne constituent pas encore explicitement une attente de premier niveau, au même titre que la disponibilité, l'intégrité ou la confidentialité.

On peut résumer cette ère de la sécurité des systèmes d'information par le concept de politique de gestion et de contrôle de la sécurité, précurseur de la préoccupation globale de qualité de confiance.

### **Sécurité des systèmes d'information de santé**

La spécificité sectorielle de la « sécurité des systèmes d'information de santé » par rapport à la sécurité générique des systèmes d'information évoquée précédemment, apparaît dans les années 90.

En effet, la spécificité du secteur de la santé, et même de la sphère santé/sociale, conduit à proposer des systèmes d'information (et des sécurités associées) appropriés, dans la mesure où les informations manipulées concernent, principalement, des acteurs ayant à la fois un rôle passif et une responsabilité non formellement impliquée : ce sont les patients, les malades, les assurés sociaux.

Le patient, le malade ou l'assuré social n'avait pas eu, jusqu'à cette époque, réellement voix au chapitre dans la construction, la validation ou l'utilisation des systèmes d'information de santé. Dans la plupart des cas, les données le concernant étaient saisies, traitées, étudiées, mises en statistiques, sans que son avis ne puisse être entendu. Alors qu'il s'agissait de données le concernant (dites « à caractère personnel ») et d'informations relatives à sa situation sanitaire (dites « à caractère médical ») ou sociale.

Ainsi, les années 90 ont vu se développer des notions et des besoins de sécurité propres à la sphère santé/sociale en général, et, plus particulièrement, au secteur médical, ambulatoire comme hospitalier. Nous développerons ces notions et besoins dans la suite de notre propos, mais citons simplement et pour mémoire : la traçabilité et l'opposabilité des actions, l'anonymisation ou la pseudonymisation des identifiants, la responsabilité des acteurs du système et, d'une manière générale, l'auditabilité du système et de sa sécurité pour une meilleure qualité de la confiance.

Que ce soit au plan national (à l'AFNOR), européen (au CEN) ou mondial (à l'ISO), des travaux de référence ont été menés dans ce sens, comme par exemple :

- l'ENV 12251 traite de l'authentification par mot de passe (cf. [8]) ;
- l'ENV 13729 traite de l'authentification par carte à microprocesseur (cf. [9]) ;
- l'ISO WD 17090 aborde la problématique des infrastructures à clés publiques sous l'angle technique du monde de l'informatique de santé (cf. [10]) ;
- le CR 13694 est un recueil des normes en sécurité informatique (cf. 'security') ou en sûreté-innocuité (cf. 'safety') vu sous l'angle de la qualité des logiciels (cf. [11]) ;
- l'ENV12924 propose une catégorisation des systèmes d'information de santé selon les niveaux d'exigences de sécurité exprimés par les établissements de santé (cf. [12]) ;
- l'ENV13606-3 aborde la problématique de partage de l'information médicale dans le cadre du dossier de santé électronique communiquant (cf. [13]) ;
- l'ENV13608-1 traite de la sécurité des communications de santé aux plans conceptuel, déontologique et normatif, propres aux attentes sectorielles (cf. [14]) ;
- le FD S 97-560 offre une méthodologie sécurité complète (glossaire, méthode, analyse et techniques) consacrée aux techniques d'anonymisation (cf. [15]) ;
- le FD S 97-700 offre une terminologie sécurité complète (glossaire, définition, homonymes et synonymes) consacrée à la sécurité dans la santé (cf. [16]).

Parmi ces normes on distingue deux finalités disjointes qui permettent de :

- raffiner partiellement des normes de sécurité génériques existantes afin de sensibiliser les acteurs du secteur santé à des questions essentielles préalables à toute démarche sécurité intelligemment mise en œuvre ; citons, par exemple, l'authentification par mots de passe ou par cartes à microprocesseur, la certification de clés publiques et la dualité entre sécurité et innocuité (cf. [8], [9], [10] et [11]) ;
- dédier à la santé, des normes de sécurité, spécifiques pour apporter aux acteurs de la santé les éléments de réponse juridiques, organisationnels, conceptuels, méthodologiques et techniques ; de façon à traiter les problématiques particulières non résolues par les diverses normes de sécurité, génériques existantes (cf. [12], [13], [14], [15] et [16]).

Sous des appellations parfois distinctes (traçabilité, imputabilité, opposabilité, irréfutabilité, non-réputabilité, responsabilité ou encore 'accountability') des normes abritent des concepts connexes ; certaines de ces normes développent cette quatrième propriété de base de la sécurité qu'est l'auditabilité, à la fois complémentaire et orthogonale à ses trois homologues : la disponibilité, l'intégrité et la confidentialité.

La propriété d'auditabilité est complémentaire car elle garantit la confiance dans les trois autres ; c'est une véritable sécurité de la sécurité. La démarche d'auditabilité permet d'attribuer aux systèmes auditables (et à leur sécurité) un certain niveau de confiance.

La propriété d'auditabilité est orthogonale car, contrairement aux trois autres, elle est applicable au système à tous les niveaux, depuis la plus petite parcelle d'information, jusqu'aux processus de plus haut niveau (organisationnels, juridiques, etc.) ; alors que les trois autres propriétés s'adressent de façon particulière, soit aux données de bas niveau, soit aux informations de plus haut niveau d'intégration voire aux processus purement informatiques.

Certaines normes présentées supra (cf. [12], [13], [14], [15] et [16]) abordent et prennent en compte aussi bien la problématique juridique des responsabilités que les problèmes techniques et organisationnels.

On peut, alors, résumer cette ère de la sécurité des systèmes d'information de santé par le concept de politique de sécurité juridico-technique. Cette politique prend en compte, à la fois, cette nouvelle dimension juridique (et donc éthique et déontologique) et la précédente dimension technique plus classique, qui recouvrait les aspects organisationnels et opérationnels de la sécurité.

### ***Sécurité des systèmes d'information et de communication hospitaliers***

La « sécurité des Systèmes d'Information et de Communication Hospitaliers (ou SICH) » est actuellement en plein essor avec le développement des réseaux ville-hôpital, la progression du dossier de santé électronique communicant, la volonté de modernisation de l'ensemble des Systèmes d'Information Hospitaliers (SIH) en coopération avec l'évolution de l'ensemble des Systèmes d'Information de Santé (SIS).

Les SICH ont le privilège de pouvoir hériter de l'ensemble des acquis obtenus à travers les diverses ères de la sécurité : sécurité informatique et des technologies de l'information, sécurité des systèmes d'information puis des systèmes d'information de santé.

À l'inverse, les SICH ont l'inconvénient majeur d'avoir l'obligation de respecter un « modèle de spécification et de fonctionnement de la sécurité » capable de prendre en compte l'ensemble des problématiques essentielles de la sécurité :

- combinant les considérations d'ordre à la fois du juridique et du technique ;
- concernant à la fois la disponibilité, l'intégrité et la confidentialité ;
- prenant en compte les rôles, fonctions, responsabilités et usages dans l'hôpital ;
- intégrant les dimensions locale (intranet) et globale (extranet) ;
- conciliant les métiers du soin (cf. innocuité) et ceux de la recherche (cf. sécurité) ;

Seule, une démarche rigoureuse et scientifique peut prétendre répondre à l'ensemble de ces exigences et à leur complexité ; il s'agit de l'activité de modélisation formelle des politiques de sécurité :

- on doit modéliser les situations réelles auxquelles seront confrontées les politiques de sécurité à définir et à mettre en place ; la modélisation analytique permet d'atteindre le système le plus pertinent et le plus réactif possible, alors que la méthode énumérative risque de ne pas être exhaustive et de ne pas pouvoir prendre en compte une situation réelle complexe ;
- dès qu'il s'agit de santé, donc d'innocuité, des préoccupations de fiabilité apparaissent ; elles peuvent être résolues par la modélisation formelle de scénarios, contextes, environnements... très souvent considérés comme n'offrant pas de perception fiable de la situation : des travaux français (cf. projet MP6) et européens (au CEN/TC251) sont en cours sur ces sujet.<sup>10</sup>

On peut résumer cette ère de la sécurité des systèmes d'information et de communication hospitaliers par la notion de modèles de politiques de sécurité, qui doivent à la fois :

- répondre aux situations courantes, habituelles et quotidiennes, qui nécessitent de respecter des besoins de sécurité - certes non négligeables et non triviaux - mais d'ordinaire facilement traités (exemple : « qui peut accéder à quoi ? ») ;
- résoudre des situations conflictuelles, inhabituelles et exceptionnelles, soulevant quelques dilemmes décisionnels ; il convient de lever impérativement ces dilemmes qui combinent 'sécurité-security' et 'sécurité-safety' (ou innocuité) en prenant en compte les responsabilités des décisions prises, en intégrant les codes d'éthique, en respectant la déontologie et les lois (exemple : en cas d'urgence et en l'absence de l'autorité compétente, comment et qui peut prendre une décision dont elle aura juridiquement à répondre ?).

## Sécurité et standardisation (méthode)

Ce chapitre explique quelques nuances essentielles à la compréhension du monde de la normalisation et des évolutions actuelles dans le secteur de l'informatique de santé.

### **Standardisation et Normalisation**

La nuance<sup>11</sup> entre l'activité de standardisation et celle de normalisation, et donc entre les standards (de facto) et les normes (de jure), est essentielle pour bien comprendre les évolutions actuelles et futures, en matière de modernisation de l'informatique de santé, en France notamment.

La standardisation correspond à une pratique, largement développée dans les années 80, encore très répandue dans les années 90 et, malheureusement, encore présente dans certains lieux à l'heure actuelle ; elle consiste à développer des « normes propriétaires » soit au sein de sa propre activité informatique, soit en amont chez les constructeurs et fournisseurs de matériels et logiciels informatiques. Les standards peuvent ensuite s'imposer comme normes ou normes sectorielles d'autant qu'ils répondent en général exactement au besoin, mais souvent à court terme et avec peu d'espérances d'évolutivité, d'interopérabilité voire de communicabilité d'un système à l'autre.

La normalisation, et en particulier, la normalisation en informatique de santé, s'appuie sur les normes existantes, lorsque cela est acceptable et pertinent, et à travailler ensuite à un consensus pour établir des référentiels et des documents normatifs qui conviennent à l'ensemble de la population concernée. Les normes répondent alors à l'ensemble des besoins de cette population mais elles peuvent courir le risque de n'être suffisamment pertinentes que pour une mineure partie de celle-ci ou pour un périmètre réduit de l'objectif initial. Ceci résulte souvent du lissage entre les exigences de différents acteurs majeurs très influents pour les normes nationales, ou entre les exigences de plusieurs pays normalisateurs ayant des besoins différents, pour les normes internationales.

---

<sup>10</sup> MP6 (MPSSICSS : Modèles et Politiques de Sécurité des Systèmes d'Information et de Communication en Santé et Social) est un projet RNRT de R&D partiellement financé par la Direction de la Technologie au Ministère de la Recherche. Son objectif de proposer des modèles formels, notamment pour l'autorisation, l'anonymisation et la non-inférence.

<sup>11</sup> Une fois n'est pas coutume : nous avons, nous autres francophones, deux termes différents (« standard » et « norme ») pour exprimer des notions distinctes (de facto et de jure), là où les anglophones n'en n'ont qu'un (« standard »).

## **Normalisation en Informatique de Santé**

La normalisation en informatique de santé, qui a pris toute son importance au milieu des années 90, est relativement récente par rapport à d'autres domaines de la normalisation de l'informatique.

Ce retard s'explique car l'informatique de santé a dû se tailler une place au sein de toutes les instances de normalisation et entre les différents domaines de la normalisation en informatique. Longtemps appelée « informatique médicale » (ou « medical informatics »), elle a été rebaptisée « informatique de santé » (ou « health informatics ») en 1996 au CEN puis à l'ISO, et ensuite « informations de santé » (ou « health information systems ») en 1998 à l'AFNOR, traduisant ainsi la volonté d'être à la fois :

- assez spécialisée vers toute la sphère santé (en l'occurrence) par opposition à la normalisation dans le domaine des technologies de l'information très généraliste ;
- peu spécialisée au seul domaine médical (en l'occurrence) vis-à-vis des nouvelles tendances qui se font jour : informatique médicale, bio-informatique, neuro-informatique et autres disciplines.

Il en va de même pour la sécurité des systèmes d'information de santé au confluent de l'informatique traditionnelle, de l'informatique médicale et de l'informatique de santé et, surtout, héritant, pour le meilleur et pour le pire, d'années d'investissements en sécurité, en sécurité informatique et en sécurité des systèmes d'information (cf. notre chapitre « Histoires de sécurité »).

L'activité de normalisation en sécurité des systèmes d'information de santé doit désormais répondre à un challenge intéressant mais audacieux :

- prendre en compte l'héritage de la généralité des approches, méthodes, techniques et solutions de sécurité développées pour la sécurité des systèmes d'information en général ; cependant elle ne doit pas en abuser sous peine de n'apporter aucune valeur ajoutée aux acteurs de la santé ;
- développer autour de cet héritage tout le corpus nécessaire des notions et concepts, des méthodes et approches, des solutions et orientations, qui sont spécifiques aux besoins et aux attentes des acteurs de la santé en matière de sécurité pour la santé.

Animateur du GE-SSIS d'AFNOR et « convenor » du WG III au TC251 du CEN, je m'attache à défendre ce point essentiel tant au plan français qu'au plan européen : ne pas prendre pour argent comptant - comme cela a trop souvent été le cas - des approches ou solutions standard, inadaptées aux spécificités du secteur concerné, surtout lorsqu'il s'agit d'un secteur à haut risque ou très sensible comme celui de la santé.

Où seraient la valeur ajoutée, l'utilité et l'intérêt de groupes de travail et de normalisation qui se contenteraient de reprendre, sous leur enseigne, des normes génériques, ou a-sectorielles, déjà applicables de fait.

Si spécificités il y a, le groupe ad hoc du secteur se doit de les exprimer et de les traiter.

## **Évolution des normes en Informatique de Santé**

Les normes développées en informatique de santé ont inévitablement suivi ce chemin (du « médical pur » à la « santé en général »). Elles sont souvent perturbées par l'apparition régulière et en progression croissante (le périmètre s'élargissant) de centres de pressions ou d'oppositions, de-ci, de-là, très souvent issus d'outre-Manche et d'outre-Atlantique. Ces perturbations compliquent fortement le processus d'obtention d'un consensus autour d'un document, norme, programme de travail, champ d'investigation ou spectre d'application.

Concernant les normes en sécurité des systèmes d'information de santé, la distinction explicitée supra entre les normes plus anciennes (cf. [8], [9], [10] et [11]), raffinant en partie des normes de sécurité génériques existantes (cf. [1], [2], [3], [4], [5], [6] et [7]) et les normes plus récentes (cf. [12], [13], [14], [15] et [16]), dédiées à la santé car nouvelles et spécifiques, traduit exactement l'évolution actuelle des normes en sécurité pour la santé.

A titre d'exemple, la norme ENV12924 [12] sur la catégorisation des protections pour les systèmes d'information de santé, actuellement en cours de révision au sein du WG III du TC251 du CEN, subit ces deux influences ; ainsi, sont à la fois exprimées :

- la volonté de prendre encore plus en compte la norme générique ISO17799 [5], qui a une finalité comparable à l'ENV12924 [12] mais avec une approche différente ;

- la nécessité de spécialiser la nouvelle version de l'ENV12924 [12] vers les besoins métier et les attentes sectorielles du monde santé et du domaine hospitalier, avec, par exemple, l'auditabilité comme nouveau critère intégré à la catégorisation.

## **Vers une meilleure prise en compte des normes (résultat)**

Ce chapitre aborde, en amont et en aval, le problème de la trop faible prise en compte des normes en général, en santé en particulier et en sécurité notamment.

En amont, le problème réside dans le faible participation des acteurs de la santé à la construction, validation et expérimentation des normes ; même si beaucoup de raisons, tantôt légitimes (disponibilité, compétences ...) tantôt non acceptables (coûts, intérêt ...) pourraient être rappelées, ce que nous ne ferons pas ici, car ce n'est ni le lieu, ni l'objectif.

En aval, le problème repose sur la très faible connaissance et la trop faible prise en compte des normes de santé, et des normes en sécurité, pour pouvoir prétendre être à jour et en règle avec le minimum vital imposé, étant donné que certaines d'entre elles s'imposent de fait, même si beaucoup de raisons, tantôt légitimes (complexité du monde des normes), tantôt non acceptables (sensibilisation à l'application des normes) pourraient être rappelées, là encore.

### ***Normes de jure plutôt que standards de facto***

Il est désormais évident et admis par l'ensemble des acteurs moteurs de la modernisation des systèmes d'information de la sphère santé, qu'il est préférable de faire appel à des normes (normes de jure), si elles existent, plutôt qu'à des standards (standards de facto).

Les normes ont l'avantage d'être une base méthodologique et technologique et un référentiel commun à tout le secteur, partageable entre tous, évolutif de par l'infrastructure des instances de normalisation, interopérable par essence et communicant avec la prise en compte, actuelle des nouvelles technologies de l'information et de la communication.

Les standards, apparus avant toute exigence d'universalité, étaient des bases de travail et référentiels techniques compréhensibles à l'époque des ordinateurs centraux, où les grands acteurs pouvaient se permettre d'imposer leur loi.

Désormais, avec l'émergence des technologies intranet, extranet et internet, avec le succès du développement des réseaux ville-hôpital, avec la réalité de l'informatisation de tout le système d'information de santé, avec la volonté de modernisation des systèmes d'information hospitaliers, avec la réaffirmation de la nécessité de participation active du patient à la connaissance et à la maîtrise de son propre dossier de santé, avec l'acceptation consensuelle du dossier de santé communicant plutôt que centralisé et du dossier médical partagé plutôt que distribué, la normalisation (très active sur ces sujets) et les normes (indispensables dans ces domaines) deviennent des outils plus consensuels et pertinents que l'ancienne standardisation avec ses standards (propriétaire ou constructeur), très vite obsolètes et générateurs de surcoûts à la moindre modification significative du contexte d'application ou la moindre évolution importante de l'environnement de mise en œuvre.

### ***Implication dans la normalisation et prise en compte des besoins sectoriels***

Mais pour cela il faudra une meilleure implication de l'ensemble des acteurs de la santé dans les instances de normalisation, tant nationales et européennes, qu'internationales. Tous, sans exception, doivent pouvoir y contribuer.

L'époque de l'expression des besoins de l'utilisateur final par l'informaticien semble révolue. Par analogie, il n'est pas acceptable que les experts en sécurité des systèmes d'information - certes de santé - influencent constamment l'émergence de normes au service du patient-citoyen en particulier quant au respect de l'anonymat. Il appartient aux plus hauts responsables des institutions de la santé et des établissements de soins de porter le discours des assurés sociaux et des patients car ils représentent leurs intérêts sanitaires, individuels et collectifs, et ils sont porteurs de leurs besoins d'informations et de respect de leur intimité.



## Tendances essentielles (discussion)

Des tendances essentielles se font jour qui concernent exclusivement le domaine que nous maîtrisons : la sécurité des systèmes d'information de santé (SSIS), en général, et, en particulier, la sécurité des systèmes d'information hospitaliers (SIH).

Les cinq paragraphes suivants détaillent ces tendances émergentes, déjà abordées par les différents groupes de normalisation en santé : sécurité et qualité, sécurité et innocuité, sécurité et intimité, anonymisation et pseudonymisation et auditabilité.

### **Sécurité et/ou Qualité**

La querelle entre la sécurité et la qualité est révolue. La sécurité, si elle est efficace, est un apport incontestable à la qualité d'ensemble du système d'information. Inversement, la qualité des données fournies, la qualité des processus mis en œuvre et la qualité des informations générées (dont celles utiles à la gestion de la sécurité) contribuent à une meilleure sécurité du système dans son ensemble.

Le débat se situe plutôt au plan des indicateurs des niveaux de sécurité et de qualité. Une solution actuellement développée consiste à s'intéresser à la « qualité de la confiance » : quels indicateurs de confiance retenir et quelle fiabilité<sup>12</sup> attribuer à ces indicateurs ?

Un groupe de travail ad hoc, créé à l'AFNOR au sein de la commission de normalisation « Sécurité des Systèmes d'Information » se penche sur cette question.

En informatique de santé, un indicateur de la confiance d'un système est son niveau de sécurité et aussi, de façon récursive, la perception que chacun a de celle-ci. La communauté de l'informatique de santé fait ainsi appel à l'auditabilité du système d'information et donc, récursivement, à l'auditabilité de la sécurité même du système (cf. [12], [14], [15] et [16] et paragraphe consacré à l'auditabilité).

### **Sécurité-‘Safety’ versus Sécurité-‘Security’**

Dans un établissement de soins dont le métier premier est de soigner et de sauver des vies, donc la sécurité au sens d'innocuité (en français) ou au sens de ‘safety’ (en anglais), il est évident que toutes les priorités majeures et les décisions importantes doivent être en faveur de la sécurité-innocuité (ou sécurité-‘safety’).

Le problème est que cette sécurité-‘safety’ dépend fortement de quelques autres aspects de la sûreté de fonctionnement, dont la sécurité-‘security’ : en effet, une atteinte en disponibilité ou en intégrité, voire en confidentialité, sur tout ou partie du système peut avoir une incidence néfaste du point de vue de l'innocuité (i.e., on peut aisément imaginer qu'une intrusion avec intention de nuire dans un dossier de santé peut coûter la vie au patient concerné).

Des travaux ont été menés au sein du WG III du TC251 au CEN (cf. [11]), ne serait-ce que pour montrer que de nombreuses normes existent, parfois a-sectorielles, qui tentent de combiner les deux sécurités (la sécurité-‘security’ et la sécurité-‘safety’) dès lors que la qualité du système repose sur des logiciels plus ou moins critiques.

Mais là encore, l'auditabilité est un argument efficace pour traiter le fait qu'un défaut de sécurité-‘security’ du système puisse avoir une incidence néfaste en terme de sécurité-‘safety’ pour le patient, même s'il s'agit parfois plus de tirer les enseignements a posteriori pour améliorer le niveau de sécurité du système pour l'avenir.

### **Confidentialité-discrétion versus Confidentialité-séclusion**

Au sein du quadruplet DICA – Disponibilité-Intégrité-Confidentialité-Auditabilité – qui constitue les fondements de la sécurité des systèmes d'information de santé, il est possible de distinguer deux formes de confidentialité qui ne l'étaient pas il y a encore peu de temps.

---

<sup>12</sup> Mais ne compliquons pas en parlant de « fiabilité de la confiance », car la confiance a pour origine étymologique la notion de fiabilité et, surtout, parce qu'une fiabilité évaluée ou mesurée, une sécurité obtenue, une confiance accordée ou une qualité constatée, s'apparentent à des perceptions différentes de la même notion de sûreté de fonctionnement.

La confidentialité classique (ici : confidentialité-discrétion) est obtenue en protégeant par des techniques réversibles (bien souvent cryptographiques) dites de chiffrement (sinon par des méthodes à base de fragmentation). Ensuite, il reste à déprotéger par des techniques cryptographiques de déchiffrement cette fois (sinon par dé-fragmentation) les informations nécessitant une certaine discrétion : ainsi, par exemple, un extrait de dossier médical échangé par messagerie sur un réseau entre deux professionnels de santé.

Avec ce type d'exigence en confidentialité-discrétion, il est toujours possible de lever la discrétion (cf. déchiffrement après chiffrement, dé-fragmentation après fragmentation) :

- soit légitimement, par cryptographie, pour l'utilisateur habilité ayant reçu autorisation d'accéder et d'utiliser la bonne clé de dé-protection (clé de déchiffrement ou de dé-fragmentation) ;
- soit illégitimement, par cryptanalyse, pour le « hacker » non habilité forçant la technique de protection utilisée (cryptographique ou autre), lorsque celle-ci n'est pas suffisamment robuste ;

La confidentialité d'un nouveau type (ici : confidentialité-séclusion) est obtenue en protégeant de façon irréversible et robuste à toute tentative d'indiscrétion, l'information sensible nécessitant plus qu'une certaine discrétion et soumise à une volonté délibérée de séclusion<sup>13</sup>. On parle d'anonymat, d'intimité, de vie privée ou, plus généralement et dans le cadre de cet article : d'intimité électronique.

Si la technique mise en œuvre pour répondre à une exigence de confidentialité-séclusion est suffisamment robuste, tant mathématiquement, que statistiquement, ou par la logique ou par cryptanalyse, alors il sera possible de « lever » la séclusion (expression antinomique), contrairement à la discrétion. C'est donc le concept idéal pour prendre en compte le respect de la vie privée, la notion de « colloque singulier » reclus entre un patient et son médecin et aussi pour garantir la non-divulgateur d'informations individuelles et à caractère médical, de soin, de santé, qu'elles soient nominatives ou même anonymes.

En sécurité des systèmes d'information de santé, tant au plan français par le document normatif auquel nous avons fortement contribué (cf. [15]) qu'au plan européen auquel un sujet de travail a été accepté depuis 2000, ces travaux de distinction entre la discrétion et la séclusion ont été perçus comme précurseurs vis-à-vis de l'identification du patient et aussi novateurs pour des secteurs autres que la santé (cf. paragraphe sur l'anonymisation).

Mais, à nouveau, s'il n'y a pas de confiance, ni d'auditabilité, sur l'efficacité d'une réelle séclusion par rapport à de la discrétion classique, cela ne sera que de peu d'intérêt.

### **Anonymisation ou Pseudonymisation**

L'anonymisation consiste à remplacer les données d'identification d'un individu et toutes les informations identifiantes le concernant par des numéros ou « identifiants » qui doivent être à la fois muets (c'est-à-dire sans sémantique) et anonymes (c'est-à-dire sans retour possible vers l'identité de l'individu) ; en contre-exemple, citons le numéro INSEE (dit « numéro de sécu. ») qui renseigne sur le sexe, la date et le lieu de naissance et est en bijection avec, actuellement, le nom de l'assuré social (Vitale1) et, à l'avenir, avec celui du patient (Vitale2).

La pseudonymisation consiste à remplacer toujours et partout (pour un contexte et un périmètre donnés, comme par exemple les statistiques du PMSI) l'identifiant d'un même individu par le même numéro ou « identifiant » anonyme dit pseudonyme : il s'agit donc d'une anonymisation toujours et partout la même, dont avec pseudonyme.

Il faut surtout avertir qu'une donnée anonymisée (ou, surtout<sup>14</sup>, pseudonymisée) n'est pas irrémédiablement anonyme : car elle reste une donnée individuelle donc à caractère personnel, et elle le restera tant qu'elle ne sera pas agrégée. Il peut paraître paradoxal de proclamer qu'« anonymisé » ne veut pas forcément dire « anonyme ». Comme le montrent toutes les techniques d'inférence

<sup>13</sup> La « séclusion » est une forme de réclusion décidée de son plein gré par l'individu concerné, lorsque celui-ci souhaite préserver son intimité vis-à-vis des agressions externes.

<sup>14</sup> Anonymisée ou, surtout, pseudonymisée : une information anonymisée (un épisode de soin des statistiques PMSI), lorsqu'elle est chaînée par le même pseudonyme anonyme avec d'autres informations anonymisées (trajectoire de soins des statistiques PMSI), devient une information corrélée (i.e. pseudonymisée) bien plus vulnérable vis-à-vis des risques de désanonymisation que lorsqu'elle était isolée (i.e., anonymisée sans être pseudonymisée).

(déductive, inductive, abductive et « adductive ») issues de la logique du premier ordre et aussi de la logique modale, il est possible de recouvrer des informations nominatives à partir de données pourtant anonymisées.

On voit là tout l'intérêt mais aussi les limites des différents avis prononcés par la CNIL – Commission Nationale de l'Informatique et des Libertés – permettant de dire que des données sont ou non nominatives, bien que demeurant toujours à caractère personnel.

Divers travaux effectués ou en cours, mentionnés précédemment (cf. [15] à l'AFNOR et sujet de travail au WG III du TC251), abordent ce sujet pour lequel il n'y a pas encore de fondement scientifique établi, alors qu'il s'agit d'un problème de société. Imaginez l'émoi si, lors de la publication par un établissement de soins, sur son site web, de ses statistiques concernant les pathologies traitées et les populations de patients soignés, un « hacker » mal intentionné, ou animé de visées mercantiles, pouvait ré-identifier la majeure partie des patients constituant toutes ces statistiques, en utilisant les différentes techniques d'inférence évoquées supra... !

### **Auditabilité plutôt que 'Accountability'**

L'auditabilité (littéralement : « capacité à être audité ») ne doit pas être confondue avec la propriété de « accountability » (dont une mauvaise traduction de l'anglais est : traçabilité).

Cette « accountability » (traduction littérale : « capacité à rendre compte ») est à rapprocher de la technique de non-répudiation issue originellement de la norme ISO 7498-2 qui s'adressait aux échanges et protocoles des couches OSI. Elle se situe surtout à un niveau technique :

- non-répudiation par l'origine d'un message de l'émission de ce message ;
- non-répudiation par la destination d'un message de la réception de ce message ;
- non-répudiation par l'origine du message de sa remise à un opérateur télécom ;
- non-répudiation par la destination du message de sa livraison par l'opérateur télécom.

L'auditabilité se situe plus à un niveau juridico-technique englobant les diverses notions techniques de traçabilité (trace d'une action), imputabilité (imputation de cette action à un rôle), et aussi les notions juridiques d'opposabilité (opposer devant un juge un élément probant), voire irréfutabilité (lors d'un jugement sur la base d'éléments probants). Avec l'apparition en Europe (directive européenne) et en France (loi, décrets et arrêtés), de la force probante de la « signature électronique » (anciennement dite « signature numérique »), ces notions juridico-techniques prennent tout leur sens dans le contexte sensible de la santé.

Évoquée à plusieurs reprises, à travers les diverses perceptions traitées dans cet article, l'auditabilité constitue l'apport majeur de l'activité en sécurité des systèmes d'information de santé. Rendre un système d'information (hospitalier, par exemple) capable d'être audité pour permettre d'en évaluer sa qualité et, similairement, rendre aussi la sécurité de ce système d'information (hospitalier, dans notre exemple) capable d'être auditée pour permettre d'en estimer sa confiance ou la qualité de cette confiance, est un plus. C'est le minimum que doit apporter la normalisation en sécurité des systèmes d'information de santé (cf. [14], [15], et [16]), à laquelle nous avons contribué depuis quelques années.

Si l'« accountability », notion pourtant sémantiquement forte (capacité à rendre compte), est devenue une propriété assez faible (restreinte à des techniques de non-répudiation), alors l'auditabilité, notion à la fois technique (reprenant en cela l'« accountability ») et juridique (innovant en cela autour de la « signature électronique »), est indispensable au développement futur des systèmes d'information de santé, des systèmes hospitaliers en premier lieu.

## **Quel avenir pour les normes en sécurité/santé (conclusion)**

De nombreux travaux normatifs ont déjà été effectués en informatique de santé et en sécurité des systèmes d'information de santé, mais il reste beaucoup à faire :

- de nouveaux chantiers sont en cours avec l'émergence de l'ISO17799, les révisions de l'ENV12924 et de l'ENV13606-3 et la probable révision de l'ENV13608-1 ;
- l'appellation « systèmes d'information et de communication » prend tout son sens dans le secteur hospitalier avec les considérations de sécurité à associer au respect de l'intimité du

patient et au colloque singulier, au dossier de santé communiquant (pas obligatoirement communiqué), au dossier médical partageable (pas systématiquement partagé), à la confiance accordée en générale aux SICH et à leurs sécurité associées.

De nombreux concepts et aspects fondamentaux, sur lesquels nous travaillons depuis de nombreuses années, ont pris leur place dans des normes nationales, européennes ou internationales et commencent à être utilisés de façon opérationnelle dans les établissements : respect de l'anonymat, anonymisation et pseudonymisation, politique de partage des informations, nécessité d'auditabilité pour les SICH et ainsi volonté de partager, avec les utilisateurs finals, la confiance placée dans de tels systèmes.

Mais encore faudra-t-il, pour que ces efforts plus ou moins aboutis perdurent, que tous les acteurs de la santé et du monde hospitalier prennent conscience de la nécessité de :

- s'appuyer sur la normalisation en santé qui est à la fois flexible et pertinente ;
- contribuer à la normalisation en sécurité pour qu'elle soit encore plus efficace ;
- s'opposer à la normalisation parfois imposée d'Outre-Manche ou d'outre-Atlantique, selon des visions souvent trop éloignées de l'éthique et de la déontologie françaises et européennes.

## Remerciements

Mes remerciements à l'ensemble des participants, experts-sécurité, professionnels de santé, ingénieurs en normalisation, fidèles et assidus [ils se reconnaîtront] aux groupes sécurité (AFNOR/CNIS/GE-SSIS et CEN/TC251/WG III) que j'ai l'honneur et le plaisir d'animer avec toute ma sincérité.

Remerciements également aux organisateurs de ce colloque qui m'ont donc permis de (faire l'effort pour trouver le temps pour) rédiger ces quelques propos, ainsi qu'aux re-lecteurs du comité scientifique qui m'ont apporté leurs précieux retours sur cet article.

Toute ma reconnaissance enfin, au comité de lecture de la Lettre ADELI, et surtout à Alain Coulon qui, comme à son habitude, a pris le plus grand soin à relire et corriger cette version de mon article pour une parution en avant première dans cette Lettre ADELI.

*Dr Gilles TROUESSIN*  
*Ernst & Young – Audit et Sécurité des Systèmes d'Information*  
*1, place Alfonse Jourdain – 31000, TOULOUSE*  
*Tél. : 05 62 15 51 36 – Fax : 01 58 47 10 33*  
*gilles\_trouessin@ernst-young.fr*

## Biographie

Gilles TROUESSIN est Docteur en Sécurité et Sûreté de Fonctionnement depuis 1991. Il s'est spécialisé dans la Sécurité des Systèmes d'Information de Santé depuis 1993 et il a été ensuite nommé expert-normalisation en Informatique de Santé en 1996, 1997 et 1998, respectivement à l'AFNOR, au CEN et à l'ISO.

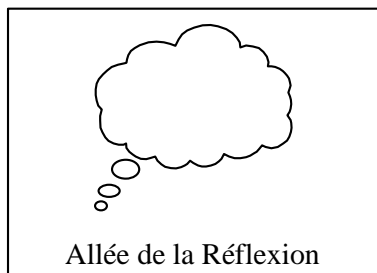
Depuis 1996, il a participé à la création, il contribue activement et, surtout, anime le Groupe d'Experts en Sécurité des Systèmes d'Information de Santé (GE-SSIS) d'AFNOR.

Depuis 1997, il participe activement au Working Group on Security Safety and Quality du Technical Committee 215 – Health Informatics au CEN – Comité Européen de Normalisation, dont il a été élu Convenor en septembre 2001.

Il participe régulièrement aux travaux du Working Group on Security et du Working Group on Health Card du Technical Committee 215 – Health Informatics de l'ISO – Organisation Internationale de Standardisation'.

## Bibliographie

- [1] ISO 7498-2:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture.
- [2] TCSEC -- Trusted Computer Security Evaluation Criteria, 1985.
- [3] ITSEC -- Information Technology Security Evaluation Criteria, 1991.
- [4] ISO 15408-1 ISO/IEC Information Technology -- Security Techniques Evaluation for IT security -- Part 1: Introduction and general model
- [5] ISO 17799 -- Code of Practice for Information Security Management
- [6] GMITS 1-5:
  - ISO 13335-1 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 1: Concepts and Models for IT Security
  - ISO 13335-2 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 2: Managing and planning IT Security
  - ISO 13335-3 ISO/IEC Information Technology – Guidelines for management of IT Security-Part 3: Techniques for management of IT Security
- [7] ISO 10181 1-7 :
  - ISO/IEC 10181-1:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview
  - ISO/IEC 10181-2:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Authentication framework
  - ISO/IEC 10181-3:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Access control framework
  - ISO/IEC 10181-4:1997 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Non-repudiation framework
  - ISO/IEC 10181-5:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Confidentiality framework
  - ISO/IEC 10181-6:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Integrity framework
  - ISO/IEC 10181-7:1996 Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Security audit and alarms framework
- [8] ENV12251 Health Informatics -- Secure User Identification for Healthcare -- Identification and Authentication by Passwords - Management and Security
- [9] ENV13729 Health Informatics -- Secure User Identification -- Strong Authentication using Microprocessor Cards
- [10] ISO WD 17090 Public Key Infrastructure
- [11] CR13694:1999 Health Informatics – Safety and Security related Software Quality Standards for Healthcare
- [12] ENV12924 :1996 Security Categorisation and Protection for Healthcare Information Systems
- [13] ENV13606-3 Health Informatics -- Electronic Healthcare Record Communication – Part 3: Distribution Rules
- [14] ENV13608-1:1999 Health Informatics -- Security for Healthcare Communication – Part 1: Concepts and Terminology
- [15] FD S 97-560 -- Fascicule de Documentation -- Informatique de Santé -- Anonymisation -- Glossaire, démarche d'analyse et expression de besoins
- [16] FD S 97-700 -- Fascicule de Documentation -- Informatique de Santé -- Glossaire – Sécurité des Systèmes d'Information de Santé



# La mémoire d'Internet

**Organisons l'archivage intelligent du contenu de la Toile !**

*Dans un numéro du quotidien « le Monde » publié en août 2002, Emmanuel Hoog, président-directeur général de l'INA (Institut National de l'Audiovisuel) nous interpelle : « Internet a-t-il une mémoire ? ». Nous reprenons et commentons les principales préoccupations exprimées dans ce « point de vue ».*

Emmanuel Hoog présente sa vision de conservateur, affronté à la nécessité d'archiver les informations nécessaires et suffisantes pour tracer la mémoire de l'humanité.

- À partir de quelques indices matériels fragmentaires, l'archéologie peut reconstituer certains modes de vie de nos lointains ancêtres.
- Des œuvres d'art (édifices, sculptures, peintures) traversent les siècles et nous apportent, entre autres, des témoignages vivants des civilisations antérieures.
- Des documents écrits, pieusement conservés dans nos bibliothèques, nous transmettent des descriptions détaillées des événements vécus par nos prédécesseurs et les états d'âme de leurs auteurs.
- La photographie conserve la vision précise, présumée objective, d'une réalité figée à un instant donné.
- Le cinéma ajoute le mouvement à l'image. Cette vision, constamment améliorée par incorporation du son, de la couleur et du relief, permet de reconstituer tous les détails de l'environnement des scènes enregistrées.

Les conservateurs ont su, en dépit des invasions, des guerres, des intempéries, préserver l'essentiel du patrimoine culturel de l'humanité. L'INA, présidé par Emmanuel Hoog, a pour mission de gérer un vaste patrimoine audiovisuel national.

Depuis une dizaine d'années, l'irruption d'Internet bouleverse le paysage de l'archivage de notre patrimoine culturel. Internet, qui affranchit notre communication des contraintes de l'espace et du temps, irrigue en permanence une large population d'internautes équipés d'un matériel largement répandu. Ce formidable moyen de création et de communication met à la portée de tout auteur, un outil qui lui permet de faire partager ses états d'âmes à l'ensemble des internautes de la planète.

Internet présente de nouvelles caractéristiques qui attirent une audience croissante d'adeptes. Cependant, ces caractéristiques séduisantes au plan individuel soulèvent de nombreuses difficultés quant à la conservation dans le temps de cette richesse informative.

Quels sont les éléments constitutifs de ce patrimoine et comment les conserver en dépit de ses caractéristiques atypiques ?

## Les caractéristiques des informations de la Toile

### **L'immatérialité**

L'information, depuis la nuit des temps, était conservée sur des supports matériels (monuments égyptiens, tablettes d'argile de l'Antiquité, manuscrits du Moyen-âge, journaux de la Révolution française, tirages photographiques du second Empire, pellicules des films des guerres mondiales, etc.). Internet a libéré l'information de sa base matérielle. L'information se propage librement sans imprégner son vecteur. Bien sûr, il est possible, ici et là, selon l'humeur de l'émetteur ou de certains destinataires d'en produire une version matérielle (impression, enregistrement sur cédérom) pour un usage personnel.

Comment choisir un support qui résiste aux épreuves du temps ?

## ***La volatilité***

Les contenus informatifs d'Internet sont extraordinairement instables. Ils ont une durée de vie très courte. L'information affichée sur un site évolue au rythme des préoccupations du propriétaire du site. Elle tombe en désuétude lorsque l'on abandonne, provisoirement ou définitivement, ce site sans que l'on prenne la peine de signaler cet état de fait aux visiteurs qui le fréquentent.

Quels états des contenus informatifs doit-on conserver ?

## ***L'instabilité technologique***

Certains messages du passé sont restés (hiéroglyphes égyptiens) et nous restent encore (écritures crétoises, rongo-rongo de l'île de Pâques) incompréhensibles car les langages dans lesquels ils étaient composés sont tombés dans l'oubli.

La rapide évolution technologique (règles de codification, langages de programmation, logiciels applicatifs) ne permet pas de garantir la pérennité de la lisibilité des messages. Des informations créées il y a une dizaine d'années sous des systèmes périmés sont inaccessibles lorsqu'on a omis de les convertir sur de nouveaux systèmes ... qui seront, eux aussi, bientôt obsolètes.

Comment protéger cette information contre la dégénérescence des clés de lecture ?

## ***L'immensité***

Comme l'univers, le contenu informationnel de la Toile est en perpétuelle extension. On découvre chaque jour des milliers de nouveaux sites qui présentent leurs informations sous des formes spécifiques (pertinence, objectivité, langage, référence culturelle, etc.).

Comment sélectionner dans cette pléthore, les informations qui méritent de passer à la postérité ?

## ***La mixité***

Internet véhicule des messages numérisés, indépendamment du média de création (textes, images fixes ou animées, sons) mais il ne réalise pas de synthèse.

Comment organiser un archivage rationnel d'une telle hétérogénéité ?

## ***L'hypertextualité***

Internet favorise un vagabondage, au fil des liens empruntés par le lecteur parmi un écheveau de possibilités. Ce circuit de consultation n'est pas neutre : toute juxtaposition d'informations engendre, chez le lecteur, une nouvelle information qui résulte de l'ordre des aiguillages empruntés.

Nous étions accoutumés à la conservation d'ouvrages linéaires. Comment présenter, pour une conservation objective, un ouvrage dont la trame est déterminée, souvent inconsciemment, par le lecteur ?

## ***L'évolutivité des objets***

Sur la Toile, les créateurs transforment fréquemment leurs objets par améliorations successives. Il est impossible de savoir si l'ouvrage que l'on consulte est achevé ou toujours en devenir.

Comment gérer en configuration les objets que l'on désire archiver ?

## **Les risques encourus**

Comprenons le malaise des conservateurs qui s'efforcent de sauver de la destruction et de l'oubli toutes les expressions de la pensée humaine.

## ***L'effacement des traces***

Si nous n'y prenons garde, dans quelques dizaines d'années, les données qui jalonnent nos progrès intellectuels auront été dispersées ; les vestiges disparates, conservés au hasard des vellétés individuelles, ne permettront plus la reconstitution le cheminement de notre pensée.

### ***La disparition de la référence***

Par analogie avec le jeu du « téléphone arabe », l'altération des données, au fil de leur transmission détériorera le message initial dont nous aurons perdu la source.

### ***La manipulation des preuves***

Les données qui transitent sur Internet sont extrêmement vulnérables aux différentes formes de malversation, ce qui ouvre la porte à toutes les perversions.

### ***La privatisation de la mémoire collective***

Certains organismes privés commencent à pratiquer des campagnes de capture des informations. On peut s'inquiéter sur les conditions de la commercialisation d'une telle marchandise confiée aux seules lois du marché.

## **Les premières tentatives de sauvegarde du patrimoine**

La Bibliothèque royale de Suède procède périodiquement à un archivage systématique du contenu des sites suédois. La Bibliothèque nationale d'Australie sollicite le dépôt volontaire.

En France, depuis plusieurs siècles, l'État, par le dépôt légal, enregistre et conserve les ouvrages intellectuels auxquels on veut bien accorder une certaine notoriété. Les autorités chargées de cette mission, adaptent leurs méthodes d'archivage aux techniques de réalisation de ces ouvrages.

## **Un défi à relever pour la gestion des connaissances**

Les contenus immatériels d'Internet sont extrêmement volatils ; leur mobilité et leur fugacité les rendent difficiles à saisir. Les limites de ces contenus, en perpétuelle extension, et leurs maillages, en fluctuation aléatoire, les rendent difficiles à enregistrer.

Depuis quelques années, le sigle KM (Knowledge Management) s'est taillé une place importante dans la terminologie des systèmes d'information. La promotion des outils qui accompagnent ce nouveau thème, laisse une place à la réflexion.

La Toile est une mine d'informations d'une richesse exceptionnelle. Cependant, la nature de ces informations soulève de nombreuses questions, quant à leur conservation, pour continuer à enrichir le patrimoine culturel de l'humanité.

La sélection, l'extraction, l'archivage, la consultation de ce fonds culturel constituent autant de véritables défis pour ceux qui font métier de tisser des liens entre générations pour catalyser le progrès des civilisations humaines.

*Alain Coulon*  
*Secrétaire d'ADELI*  
*d'après un texte d'Emmanuel Hoog*