



La DSI prend-elle en compte la conformité aux lois et réglementations ?

C'est une question que les consultants et les auditeurs posent souvent aux responsables des directions des systèmes d'information (DSI). Mais c'est un sujet qui ne passionne pas les équipes informatiques et les réponses sont souvent négatives. Pourquoi ? Le sujet lui-même, la conformité, n'est pas un domaine habituel de préoccupation. Les *aspects légaux*, à l'exception de ceux concernant les contrats commerciaux, ne sont pas des thèmes métier traités par les informaticiens. Mais il y a des exceptions. Ce sont les entreprises dont certaines applications les obligent à se conformer aux *obligations de conformité* aux lois (signature électronique, LCEN¹, CNIL, etc.) ou réglementations professionnelles (IFRS, Bâle II, plan de reprise d'activités, etc.). La facturation électronique² et l'anonymisation d'informations personnelles représentent deux exemples de ces contraintes.

L'importance des réglementations dans le domaine de la conformité ne doit pas être sous-estimée. La *crise financière mondiale* actuelle montre que l'absence (ou le nombre limité) de règles internationales dans les activités bancaires peut conduire des établissements financiers (banques, assurances, etc.) et même des pays (Islande, Hongrie) à de graves situations. Des mesures énergiques et coûteuses (plans de soutien bancaire) viennent d'être décidées par les gouvernements de la plupart des pays. Mais elles ne seraient que des solutions transitoires si des *réglementations* n'étaient élaborées et mises en place.

Rappelons que la conformité aux réglementations est devenue une *exigence internationale* forte, les régulateurs demandant aux sociétés de faire preuve de plus de transparence et plus d'éthique. Le non-respect des textes des lois et règlements peut coûter cher à la société et à ses dirigeants. Les contrôles des autorités administratives peuvent être redoutables, leurs pouvoirs d'investigations et de sanctions étant notoires.

Mais quelles sont les méthodes informatiques de mise en conformité ? Plusieurs domaines peuvent servir de base, dans une première approche.

La *communication préalable de documents* est une forme d'interrogatoire légal, un moyen permettant aux parties opposées dans un procès de trouver des preuves admissibles. C'est le processus qu'utilisent les avocats pour obtenir des preuves d'une entreprise ou d'une personne afin de soutenir une action juridique, administrative ou réglementaire. Comme complément indispensable, *l'e-discovery* correspond tout simplement à l'extension du processus de communication préalable (discovery) à des informations stockées sur supports numériques. Elle comprend des courriels, des documents et autres contenus stockés sur des serveurs de fichiers, PC ou sur une variété d'autres dispositifs de stockage.

Mais tout le monde espère que le jour où l'un de ces documents ou courriels sera réclamé (par exemple pour un audit), on se rappellera encore le nom du fichier, on saura le localiser sur une des sauvegardes (palliatif habituel !), on pourra lire la bande et ré-exploiter le fichier dans un « délai raisonnable ». La vérification du bon fonctionnement de cette hypothèse est rarement faite dans les conditions d'un test de communication préalable de preuves. Nous pensons que cette approche entraînera un *surcoût* et une insuffisance de résultats probants.

¹ LCEN : Loi sur la confiance dans l'économie numérique

² Editorial du n° 29 de Perspectives



En contrepartie, pour résoudre les problèmes informatiques, il convient, par exemple, de faire l'*inventaire* des ressources informationnelles de conformité, réduire le volume de données stockées par un *filtrage du contenu*, et traiter les messages électroniques et les fichiers bureautiques au moyen d'un *archivage sélectif*. Mais ces activités ne peuvent être conduites que dans le cadre d'une collaboration entre les équipes juridique et informatique, et après avoir convaincu les utilisateurs internes d'archiver les données utiles. Ce n'est qu'ensuite que la DSI peut quasi-automatiser les différents processus.

Notons que le *courriel* envoyé ne constitue pas une preuve formelle en soi (car en droit nul ne peut se constituer ses propres preuves) mais il a une valeur juridique lorsque la preuve « pourra être faite par tous les moyens ». En revanche, le courriel reçu pourra être produit en preuve. Bien entendu, la valeur du courriel restera conditionnée par le point de vue du juge, d'où l'importance de bien conserver les 'en-têtes' qui contiennent le routage du courriel, c'est-à-dire son origine, son heure d'envoi et l'adresse IP de l'expéditeur.

L'e-discovery représente aujourd'hui 35% du coût total du contentieux, et les entreprises qui ne parviennent pas à produire des e-mails à temps ou de manière appropriée risquent des *sanctions* et de payer des amendes lourdes, sans parler des pertes de revenus et d'image de l'entreprise.

Or, plus généralement, nous constatons aujourd'hui que peu d'informaticiens connaissent la *loi du 13 mars 2000* pour « l'adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ». Elle affirme que l'écrit sous forme électronique - quels que soient son support et son mode de transmission - a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à garantir l'intégrité (scellement physique ou logique, traçabilité). Deux conditions doivent être remplies : l'écrit sous forme électronique doit être signé électroniquement et doit être archivé.

En conclusion, les entreprises sont confrontées à des réglementations abondantes qui concernent de plus en plus les systèmes d'information. Des solutions informatiques sont nécessaires. Mais quels processus utiliser pour minimiser l'impact des évolutions permanentes des réglementations ? Quelles technologies exploiter pour éviter de relancer un projet spécifique à chaque nouvelle loi ? Une *infrastructure de gestion informatique de la conformité* doit être mise en place. Elle correspond à un ensemble de moyens (technologies, processus et procédures) permettant d'adapter de façon continue le système d'information aux changements de lois et réglementations, et d'apporter les informations nécessaires aux audits et contrôles de conformité.

Une *bonne pratique* de ce type doit permettre aux DSI de mieux répondre aux contraintes légales et réglementaires.