PAGE RÉALISÉE AVEC ALAIN BENSOUSSAN, AVOCAT

La responsabilité du DSI

COMPÉTENCES JURIDIQUES. **L'omniprésence des technologies de l'information dans l'entreprise multiplie les risques juridiques encourus par le DSI. Il est responsable de tout ce qui touche à la sécurité des systèmes d'information.**

Une inflation de textes. Aujourd'hui, le périmètre de connaissance du directeur des systèmes d'information, ou DSI, va bien au-delà de l'informatique pure. Il s'étend aux compétences associées aux échanges de données via l'utilisation de nouvelles technologies de l'information dans l'entreprise.

Le DSI doit donc être associé à l'utilisation de ces nouveaux moyens d'échange au sein de l'entreprise et posséder un minimum de connaissances juridiques en ce domaine. Il lui appartient, notamment, de savoir quels sont ses droits et obligations, quel est le contour du droit des technologies de l'information, quels sont les contrats auxquels il sera confronté dans son activité, et quelles sont les règles qui s'appliquent à la vie privée et aux données nominatives circulant au sein de l'entreprise. Mais aussi quelle peut être sa responsabilité en matière de sécurité. Or, depuis la fin 2001, on ne compte plus les lois dont le sujet est la sécurité, qu'il s'agisse de la loi sur la sécurité quotidienne, celle pour la sécurité intérieure, la sécurité financière, ou encore la cybercriminalité. Et tout cela, en ne tenant compte que des réglementations nationales. On peut donc y ajouter les obligations imposées par Sarbanes-Oxley, outre-Atlantique, pour toute entreprise cotée[*] et par Bâle II, en Europe, pour les établissements financiers.

Des risques sans cesse étendus. Le DSI se retrouve donc au cœur de la sécurité du système d'information de l'entreprise. Or, la sécurité technique participant de la sécurité juridique, le DSI doit donc disposer d'un minimum de connaissances juridiques en ce domaine. Parmi les principaux gisements de risques figurent les traitements de données à caractère personnel, les droits d'auteur, la contrefaçon, et les usages illicites des outils de l'entreprise par les salariés.

D'autre part, le nombre croissant de contraintes légales en matière de sécurité (LSF [loi de sécurité financière], Sarbanes-Oxley, Informatique et libertés, etc.) et les nouvelles méthodes de partage de l'information (portables, liaisons Wi-Fi, ports USB, etc.), qui rendent plus perméable le système d'information, augmentent toujours plus la responsabilité du DSI. Cette responsabilité croissante au niveau technique s'accompagne également d'une responsabilité plus importante au niveau juridique. ●

[*] *Lire la page juridique de* 01 Informatique *du 14/10/2005.*

LES FAITS SAILLANTS

Responsabilité effective

- Le transfert des responsabilités, civiles ou pénales, est possible à l'égard du DSI. Mais la validité d'une telle délégation est conditionnée à un certain nombre de critères cumulatifs, fixés par la jurisprudence. A savoir que le titulaire d'une délégation de pouvoirs doit être pourvu de la compétence, de l'autorité et des moyens nécessaires – sur le plan tant matériel qu'humain, financier, ou technique.

LA TENDANCE

La contractualisation des relations de travail

- Le DSI doit connaître les principaux axes juridiques qui s'imposent à l'activité qu'il mène dans l'entreprise. Qu'il s'agisse du droit de la sécurité des SI ou celui des contrats à l'égard des partenaires externes de l'entreprise ou avec les membres de l'entreprise, par le biais de contrats de travail ou de chartes d'utilisation des moyens d'information et de télécommunication mis à la disposition des membres de l'entreprise.

À RETENIR

- Ne pas mettre en danger l'entreprise en gérant au mieux le système d'information et en ayant une connaissance des principaux axes juridiques qui s'imposent à son activité.
- Avoir une gestion du risque et de sa responsabilité par la prévention et la mise en place de chartes de bonne conduite des salariés concernant l'utilisation des systèmes d'information mis à leur disposition :
  – la charte, qui peut être annexée au règlement intérieur, peut être complétée par des livrets de procédure de sécurité afin d'organiser la traçabilité des incidents, le contrôle, et la conservation de la preuve numérique ;
  – elle doit prévoir explicitement toutes les interdictions en matière d'utilisation de l'internet sur le lieu du travail sous peine de voir la responsabilité de l'employeur engagée au plan judiciaire[*].
- La charte de bonne conduite doit être élaborée sous la validation des équipes juridiques pour la conformité aux obligations légales.

[*] *Lire la page juridique de* 01 Informatique *du 04/05/2006*