

QUELLES RESPONSABILITES DU FAIT DU SYSTEME D'INFORMATION ?

Isabelle Renard
Avocat associée
AUGUST&DEBOUZY

QUELS ACTIFS RESIDENT SUR LE SYSTEME D'INFORMATION ?

- Les bases de données contenant des informations sur les personnes (salariés, clients)
- Les informations techniques : savoir faire, R&D (pharmacie), logiciels, éléments brevetables
- Les informations financières (de la DAF)
- Les informations stratégiques confidentielles : stratégie de croissance, acquisition, etc...

RISQUES ET RESPONSABILITES

Le SI n'est pas un simple outil dont le management de l'entreprise peut se désintéresser. C'est devenu **l'épine dorsale** de toutes les entreprises modernes, sur laquelle repose toute leur richesse économique (Cf réflexions suite aux événements du 11 septembre).

Les média relèvent la méconnaissance profonde des dirigeants sur les conséquences d'un problème de sécurité du SI, notamment des dirigeants de PME

Origine du risque :

Externe (piratage, virus, espionnage économique), et interne (malveillance, maladresses)

La nature du risque :

Une détérioration ou un vol des actifs qui résident sur le système d'information : fuite de fichiers clients, fuite d'informations confidentielles, perte de savoir faire, attaque ciblée de la société, etc...

Ces événements peuvent avoir un impact sur l'entreprise elle même (du fait d'une perte de valeur), ou causer un dommage à des tiers : dans tous les cas, ils peuvent générer une mise en cause de la responsabilité de l'entreprise ou de certaines personnes au sein de celle-ci.

La répartition de la responsabilité

Rappel préliminaire de quelques principes généraux : responsabilité contractuelle/délictuelle, lien de causalité, évaluation du préjudice

Schéma des responsabilités :

	Resp civile	Resp pénale
Entreprise	Par tiers ayant subi un dommage	Oui (cas)
Dirigeant	Rare (faute de gestion) par actionnaire	Oui (cas)

DSI	Non	Oui si délégation de pouvoir
Salarié	Non, mais recours disciplinaire de l'employeur	Non

Conclusion : L'émergence de la notion du « bon père de famille » en matière de système d'information.

Exemples dans la jurisprudence de sanctions de celui qui ne se comporte pas en « bon père de famille » :

La récente condamnation de Lucent Technologies (TGI Marseille, 11 juin 2003), pour avoir omis de préciser dans sa charte internet que le salarié n'avait pas le droit de créer de pages personnelles à partir des moyens informatiques mis à sa disposition par l'entreprise (en l'occurrence, la salarié avait mis en ligne des contenus diffamatoires à l'encontre d'une autre société).

L'affaire « Kitetoa » (CA Paris 30 octobre 2002), où la société Tati s'est vue expliquer qu'il ne fallait pas se plaindre de ce qu'un hacker malicieux ait pénétré son système d'information pour y détourner des fichiers contenant des données personnelles de clients, puisque ces données étaient accessibles via le site internet de la société ...

Derrière ces décisions se dessine une nouvelle notion : celle du « bon père de famille » des temps modernes, qui est conscient de la nécessité d'assurer la sécurité du système d'information de son entreprise, et qui pour ce faire met en place les moyens humains, financiers, et organisationnels nécessaires.

COMMENT GERER SON SI EN « BON PERE DE FAMILLE » ?

La connaissance du risque

La première chose à faire est de savoir ce qu'il y a dans le SI de l'entreprise, ce qui permet :

- d'en connaître la valeur ;
- d'évaluer la perte pour l'entreprise en cas de détérioration ou vol de l'actif considéré.

Les mesures qui seront en suite mises en place devront être proportionnées au risque encouru pour chaque type d'actif considéré.

Une feuille de route, en huit points :

1 - La surveillance des salariés

Surveiller l'activité de ses salariés sur le réseau internet n'est pas seulement une possibilité pour les entreprises. C'est un véritable devoir, faute à se montrer gravement négligent au regard de la protection de l'entreprise et de la responsabilité de celle-ci.

La « charte internet », qui, plus qu'un guide de bonne conduite, est un véritable contrat qui décrit les droits et les obligations de chacun au regard de l'utilisation des moyens informatiques et réseau de l'entreprise.

La mise en œuvre d'une telle charte soulève beaucoup de questionnements de la part de ceux qui en ont la charge : est-ce que je peux, est-ce que je dois, et comment faire, dans cet imbroglio de recommandations et de décisions apparemment contradictoires ? Il nous semble que certaines solutions commencent à se dégager, qui certes ne sont pas parfaites – il s'agit encore d'un domaine très nouveau – mais permettent de mettre en œuvre un document efficace et utile. Nous vous livrons ici trois principes qui sont à notre sens fondamentaux :

Premier principe : transparence et discussion collective

Nous parlons à l'instant d'un « contrat », qui fixe les droits et les obligations de chacun en matière d'utilisation des moyens informatiques de l'entreprise. Mais attention, il ne s'agit pas d'un avenant au contrat de travail, qui, imposé alors que le salarié est déjà en état de subordination, aurait une valeur bien faible en cas de litige.

La charte doit porter à la connaissance de l'ensemble des salariés de façon transparente les mesures de contrôle qui sont exercées à leur égard, conformément à l'article L121-8 du Code du Travail.

Elle doit de plus faire l'objet d'une discussion avec les organes représentatifs du personnel, et être ensuite annexée au règlement intérieur de l'entreprise. Ses dispositions seront alors opposables aux salariés, et leur violation pourra le cas échéant fonder des mesures disciplinaires.

Second principe : précision et mesure

Interdire totalement aux salariés l'accès à internet pour des fins autres que professionnelles est à notre avis plus dangereux qu'autre chose car, au regard tant de la jurisprudence récente que des positions de la CNIL, il est peu probable qu'un tribunal retienne que cette interdiction soit justifiée. Tout salarié dispose d'une sphère d'intimité à son lieu et son temps de travail et, de la même façon que l'utilisation à des fins personnelles du téléphone est tolérée, celle de l'internet doit l'être aussi.

Pour autant, il faut en fixer les limites, et le faire de façon précise : interdiction de participer à des forums ou à des chats, interdiction de créer des pages personnelles, interdiction d'accéder à tout site illicite ou à caractère pornographique, respect de la propriété intellectuelle, interdiction d'installer des logiciels piratés ou non autorisés par la DSI...

De la même façon, les salariés seront informés des diverses mesures de surveillance et de filtrage mises en place par la DSI : blocage des fichiers supérieurs à une certaine taille, veille des sites visités, mesure du temps passé sur internet ...

Troisième principe : définir clairement la procédure relative aux messages « privés »

Au prétexte que les e-mail « personnels » seraient assimilables à de la correspondance privée, l'entreprise ne pourrait pas les ouvrir, faute à se rendre coupable de l'infraction de violation des correspondances. Cette position est à notre sens parfaitement irréaliste : il suffirait que le salarié accompagne son message de la mention « personnel » pour envoyer en toute impunité à un concurrent de l'entreprise par un simple e-mail tous ses fichiers clients et quelques autres informations stratégiques !

L'entreprise doit pouvoir surveiller toute correspondance qui transite par le réseau qu'elle met à disposition de ses salariés, charge à ceux ci, exerçant leur bon sens, de ne pas faire transiter sur un réseau qui est de toutes façons ouvert à tous vents des informations de nature privée et confidentielle.

Le vrai problème, qui a bien été vu par la CNIL, est plutôt de régir le statut des administrateurs systèmes qui sont amenés à avoir connaissance de ces messages. Il faut en effet éviter que ceux-ci, soumis à la pression de leur hiérarchie, ne se voient obligés de dévoiler des informations qui n'ont aucun rapport avec l'activité professionnelle du salarié mais pourraient être utilisées à son encontre (informations sur son état de santé par exemple).

Les administrateurs systèmes doivent donc :

- recevoir des instructions précises concernant les messages dont ils peuvent faire état à d'autres membres de l'entreprise : seuls les messages ayant un rapport avec l'activité professionnelle ou les intérêts de l'entreprise sont dans ce cas, et l'on conçoit bien qu'il y a là une petite difficulté dans la mesure où une telle appréciation peut se révéler très subjective ;
- d'autre part être protégés, de sorte à ne pas pouvoir faire l'objet de sanctions disciplinaires s'ils refusent, dans le cadre défini précédemment, de divulguer certains messages à leur hiérarchie. Le sujet est évidemment là aussi très délicat, compte tenu du lien de subordination de l'administrateur système à l'entreprise qui l'emploie. Néanmoins, et en attendant que celui-ci bénéficie d'une protection légale (ce qui devrait à notre avis être le cas à terme), une protection contractuelle efficace peut être organisée.

2 - La lutte contre le piratage

Le piratage, ou contrefaçon de logiciel, est une infraction pénale. Comportement fréquent au sein des entreprises où les salariés installent des logiciels piratés sur leurs postes : nécessité de mise en place d'une surveillance systématique.

3 - La mise en œuvre de la sécurité du SI :

a) par des outils techniques (logiciels anti virus, etc ...)

La presse se fait régulièrement l'écho des sommes folles qui seraient englouties dans la sécurité informatique sans que des résultats tangibles se fassent vraiment sentir. Les dépenses moyennes des entreprises en matière de sécurité se situeraient, selon les sources, entre 5 et 10% du budget informatique, mais il semble que ce soit plus en réaction à un événement déjà passé qu'en prévention.

Il s'agit donc d'un marché peu mature mais pour autant il ne faut pas rester sans rien faire : de bonnes pratiques, qui définissent un référentiel d'état de l'art à un moment donné, commencent à se mettre en place, et il est essentiel de les connaître et de les suivre.

b) par des moyens d'organisation

Peu de personnel est affecté à la sécurité au sein des DSI, et la formation et la sensibilisation des salariés de l'entreprise aux problèmes de sécurité est encore très insuffisante.

c) par des moyens juridiques :

contrôle des partenaires, notamment :

- PME sans visibilité sur la sécurité informatique (par des audits) ;
- partenariats externalisation vers low costs (risque de perte de contrôle, difficultés d'exequatur)
- tous partenariats contractuels (importance contrôle maîtrise d'ouvrage) de la relation, budget de 10% pour contrôler la relation)

4 - L'identification/authentification des personnes

Il est indispensable de savoir identifier et authentifier les personnes qui utilisent le réseau de l'entreprise ou accèdent à l'entreprise par le réseau.

Modification juridique dans tous les pays industrialisés pour reconnaître la preuve numérique. Une démarche de sécurisation passe maintenant nécessairement par l'utilisation d'outils d'identification fiables (notamment PKI).

5 - La protection juridique de la PI de l'entreprise ; dépôts, séquestre

Le DSI doit identifier les gisements d'actifs sur lesquels l'entreprise doit pouvoir prouver qu'elle détient des droits en cas de conflit : nécessité de faire appel à des tiers séquestres, dans un cadre contractuel adapté.

6 - La gestion sociale :

Le système d'information est un outil qui n'est pas neutre en terme de gestion sociale. Le code du travail contient de nombreuses obligations qui touchent au système d'information, assorties de sanctions pénales, notamment au regard :

- des traitements de données du personnel ;
- de l'introduction de nouvelles technologies dans l'entreprise
- et bien sûr de surveillance des salariés (Cf supra)

7 - La préservation du capital humain

Attention au recours extensif à la « régie », que ce soit vis à vis de SSII locales ou étrangères. Les personnels considérés peuvent entraîner des pertes de savoir faire considérables lorsque l'entreprise s'en sépare, ce qui est dramatique pour les entreprises des pays industrialisés, dont le seul véritable atout sera à court terme la capacité d'innovation.

Donc, nécessité d'une politique de ressources humaines cohérentes et de contrôle de la régie.

8 – L'archivage des enregistrements numériques

20 novembre 2003

La mémoire de l'entreprise est dans ses archives numériques. Certaines font l'objet de contraintes légales (archives fiscales et comptables) mais pas d'autres.

En particulier, ne faut-il pas confier les archives numériques à un tiers dont c'est le métier pour constituer des preuves numériques valables ?