mai
2005

GUIDE SSI
Connaître la législation en vigueur et la jurisprudence

Fiche 2

MEDEF

Accompagner

Quel est le régime général de responsabilité applicable ?

■ **La responsabilité civile de l'entreprise (art. 1384 alinéa 5 du code civil)** : l'employeur est civilement responsable du fait de l'activité de ses préposés, notamment en cas d'utilisation malveillante des moyens informatiques et de communications électroniques (ex : messagerie, forums)

■ **La responsabilité pénale de l'entreprise** : l'employeur peut être pénalement responsable du fait de ses préposés dès lors qu'ils commettent des infractions susceptibles d'engager la responsabilité pénale des personnes morales (ex : atteinte aux systèmes de traitement automatisé de données, contrefaçon…) et qu'elles ont été commises pour le compte de l'entreprise par ses « organes ou représentants » (article L. 121-2 du code pénal).

Quelles sont les règles concernant les contenus informationnels ?

■ **Les règles en matière de données personnelles**. La loi Informatique et Libertés du 6 janvier 1978 impose au chef d'entreprise de prendre le plus grand soin des données personnelles collectées auprès de clients comme de salariés. De façon générale, les droits garantis des personnes dont les données sont traitées sont :

- Le **droit à l'information préalable**
- Le **droit d'accès** aux données traitées qui les concernent
- Le **droit de rectification** de ces données
- Le **droit de s'opposer au traitement** de ces données (collecte, utilisation, diffusion)

Sauf cas particuliers, le chef d'entreprise a l'obligation d'effectuer une déclaration préalable de ces traitements auprès de la CNIL.

L'article 34 de la loi du 6 janvier 1978 précise que le responsable du traitement est tenu de prendre *« toutes précautions utiles »* pour protéger les données à caractère personnel sous sa responsabilité, notamment, pour *« empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »*.

S'il ne respecte pas ces obligations, le chef d'entreprise s'expose à des sanctions pénales (art 226-16 à 226-24 du code pénal) et civiles.

■ **Les reproductions ou représentations non autorisées d'un contenu informationnel protégé**. La responsabilité du chef d'entreprise peut également être engagée si ses préposés utilisent dans le cadre de leur mission des logiciels « piratés ». De même, la responsabilité du chef d'entreprise peut être engagée dans l'éventualité où ses préposés utiliseraient les ressources informatiques de l'entreprise pour stocker et/ou rendre accessibles des contenus protégés (logiciels, musiques, films etc.).

■ **Le secret des correspondances privées**. Le chef d'entreprise doit veiller au respect du secret des correspondances privées, électroniques ou non au sein de son entreprise.

■ **Précaution recommandée** : Le chef d'entreprise doit prendre les plus grandes précautions en matière de surveillance par la mise en place d'une charte d'utilisation des moyens informatiques et des communications électroniques (voir fiche 4 et rapport Cyber-Surveillance sur les lieux de travail www.cnil.fr).

Quelle est la responsabilité du chef d'entreprise quant à son activité sur l'Internet ?

■ **Identification de l'entreprise sur son site Internet**. Sous peine de sanction pénale, le cybercommerçant est tenu d'assurer la mise à disposition du public *« un accès facile, direct et permanent utilisant un standard ouvert »*, aux informations suivantes :

➔ **Coordonnées de l'entreprise et de ses responsables** : sa dénomination ou raison sociale ; l'adresse de son siège social ; un numéro de téléphone et une adresse de courrier électronique où il est possible de joindre la société ; son numéro d'inscription au registre du commerce; son capital social ; le nom du directeur de la publication ; information sur les prix (frais de livraison).

➔ **Coordonnées du prestataire hébergeant le site sur l'Internet** : raison sociale, adresse et numéro de téléphone (ou mention que le site est hébergé sur les propres serveurs de l'entreprise) ;

➔ **Taxe sur la valeur ajoutée** : numéro individuel en application de l'article 286 ter du code général des impôts, numéro individuel d'identification ;

➔ **Profession réglementée** : la référence aux règles professionnelles applicables, son titre professionnel, l'Etat membre dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite ; si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci.

■ **La publicité par voie de courrier électronique doit être identifiée** : le titre du message doit suggérer son caractère publicitaire, l'identité de la société émettrice doit être indiquée, le destinataire du message doit disposer de la possibilité effective de s'opposer à l'avenir à la réception de tels messages (droit d'opposition ou opt-out). L'entrepreneur en ligne doit recueillir le consentement préalable des personnes physiques qu'il compte prospecter directement par systèmes automatisés d'appel, télécopieurs ou messages électroniques sauf exceptions posées par la loi. Tout manquement au consentement préalable peut être pénalement sanctionné (à l'heure actuelle, 750 EUR d'amende par message)

■ **La conclusion de contrats en ligne est soumise à l'article 1369-1 et suivants du Code civil** :

- L'offre doit présenter les étapes à suivre pour la conclusion du contrat ;
- L'offre doit préciser si le contrat est archivé et accessible après sa conclusion ;
- L'offre doit fournir les moyens de corriger les erreurs commises dans la saisie des données ;
- L'offre doit indiquer les langues proposées pour la conclusion du contrat ;
- L'offre doit préciser les règles professionnelles auxquelles l'auteur de l'offre entend se soumettre.

L'acceptation de l'offre par le client se manifeste par un geste électronique (le clic) ou par l'utilisation d'un procédé de signature électronique au sens de l'article 1316-4 du Code civil. Le législateur a posé une présomption de responsabilité à l'égard du commerçant en ligne concernant la bonne exécution des obligations résultant du contrat.

Que faire en cas d'attaque ?

L'entreprise peut être victime d'une « attaque » contre son système d'information (voir Guide et fiche 1).

Elle doit en ce cas :

■ **Prendre toutes les mesures permettrant de conserver la preuve des faits dont elle est victime** :

➔ faire une copie physique du disque dur concerné (image) qui sera stockée sur un support différent ; isoler sur un autre support le fichier de journalisation (log) concerné, si possible après l'avoir daté et signé électroniquement ;

➔ faire procéder à un constat des opérations effectuées par un huissier de justice.

■ **Alerter les instances de sécurité des réseaux** : informer le CERT-IST (le CERT-IST recueille et diffuse les alertes pour les entreprises de l'industrie des services et du tertiaire)

9, rue du Président Allende - 94 526 Gentilly Cedex
Tel. : 05 34 35 33 88 - Fax : 05 34 35 33 89
cert@cert-ist.com

■ **Déposer une plainte pénale** :

➔ Des dispositions du Code pénal (articles 323-1 et 323-7) sanctionnent les atteintes aux systèmes de traitement automatisé de données (STAD) telles que par exemple l'intrusion dans le système d'information, l'altération de son fonctionnement…

➔ Prendre contact avec le **SRPJ** ou la **brigade de Gendarmerie** du lieu des faits objets de la plainte (par exemple lieu du serveur attaqué) ;

ou **l'OCLCTIC** : (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) Compétence nationale - 11, rue des Saussaies - 75800 Paris- Tél: 01 49 27 49 27 - Fax : 01 49 97 80 80 ;

ou le **BEFTI** : (Brigade d'enquêtes sur les Fraudes aux Technologies de l'Information) Compétence sur Paris et la petite couronne - 163 avenue d'Italie - 75 013 Paris - Téléphone : 01 40 79 67 50

Quelles sont les exigences de la loi de sécurité financière du 1er août 2003 (LSF) en matière de sécurité des systèmes d'information des entreprises ?

La LSF a introduit dans le code de commerce les articles L. 225-37 et L. 225-68 qui prévoient pour les sociétés anonymes, que leur président du conseil d'administration ou du conseil de surveillance doit rendre compte dans un rapport spécifique *« des conditions de préparation et d'organisation des travaux du conseil ainsi que des procédures de contrôle interne mises en place par la société »*.

Ce rapport annuel devra notamment exposer les procédures de contrôle interne concernant la sécurité du système d'information de l'entreprise, garantie notamment de l'intégrité des informations comptables qu'il traite. Aux termes de l'article L. 225-235 du code de commerce, le commissaire aux comptes devra, quant à lui, dans un rapport distinct de son rapport de certification des comptes annuels, présenter ses observations sur *« les procédures de contrôle interne qui sont relatives à l'élaboration et au traitement de l'information comptable et financière »* décrites dans le rapport spécifique du chef d'entreprise.

Il est à noter que des mesures du même ordre sont également prescrites par la loi américaine Sarbanes-Oxley du 29 août 2002 mais ne concerne que les entreprises cotées aux Etats-Unis.