

# Société pour la gestion du personnel

## S E P

Section neuchâteloise

Procès-verbal N° 307

Séance du 1<sup>er</sup> avril 2003, Hôtel Beau-Rivage, Neuchâtel

**Présents** : 31

### **Thème** : PROTECTION DES DONNÉES ET FONCTION RH

Madame Chantal Cornaz, membre du comité, présente les orateurs de la soirée, M. Pierre Matile, avocat, CJE (Conseiller juridiques entreprise) et M. Denis Collé, Directeur, Profil Management, Conseil en Droit du Travail, Conseil en organisations, qui vont mener le débat à tour de rôle.

### **1. LA LOI SUR LA PROTECTION DES DONNÉES / LPD**

La LPD, en clair Loi sur la protection des données – est si vaste, qu'on ne saurait en faire le tour ce soir. Les orateurs se proposent donc, dans la partie et l'espace temps qui leur sont dévolus, de parler de cette fameuse LPD en rapport avec la gestion des Ressources Humaines en entreprise.

Cette loi sur la protection des données, loi fédérale du 19 juin 1992, est entrée en vigueur le 1<sup>er</sup> juillet 1993. Elle a une portée générale et concerne un vaste champ d'action.

### **2. QUI EST SOUMIS À CETTE LOI ?**

La constitution fédérale du 18 avril 1999 (donc plus récente que cette loi) consacre un droit fondamental de l'individu, sans distinction aucune, en son art. 13, à savoir : « Toute personne a droit au respect de sa vie privée et familiale. Toute personne a le droit d'être protégée contre l'emploi abusif des données la concernant. » Il s'agit là d'un droit universel qui ne supporte pas de discrimination, droit qui s'applique à toutes les formes de transmission de l'information. En outre, tout abus est répréhensible. Sur la base de cette règle fondamentale, s'appuient d'autres textes notamment :

- 1.Art. 28 du Code Civil Suisse : « Celui qui subit une atteinte illicite à sa personnalité peut agir en justice pour sa protection contre toute personne qui y participe. »
- 2.Art. 328b du Code Civil Suisse : « L'employeur ne peut traiter des données concernant le travailleur, que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. »

En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables. Tout ça va déboucher sur cette fameuse loi sur la protection des données, elle-même qui régleme le traitement de données personnelles par des personnes privées, notamment les informations que les employeurs traitent au sujet de leurs employés. Dans ce cadre, est soumis toute personne (privée ou publique) qui traite des données personnelles de tiers. Encore faut-il savoir ce qu'on entend par : données personnelles et traitement des données.

**Définitions** : C'est une des rares fois où la loi elle-même consacre tout un article pour expliciter les termes employés. Il faut se référer à l'art. 3 LPD.

**Données personnelles** : « Toutes les informations qui se rapportent à une personne identifiée ou identifiable ». Quand la personne est identifiée, la question ne se pose plus. Mais quand, une personne est-elle identifiable ? Ex. : une personne assiste à un séminaire interne sur le certificat de travail, par ex. L'organisateur prend dans les dossiers du personnel des certificats au hasard et les caviarde. Il fait bien attention à ce que les groupes de travail ne se penchent pas sur le certificat d'un membre du groupe. Il se peut que la personne se fasse tout de même reconnaître. Le pseudonyme n'est pas un gage d'anonymat. Les cartes de fidélité des grands magasins ? permettent un marketing ciblé en fonction des habitudes d'achat.

**Données sensibles** : Ce sont d'abord des données personnelles, mais en plus elles concernent :

- les opinions ou activités religieuses, philosophiques, politiques ou syndicales ;
- la santé, la sphère intime ou l'appartenance à une race ;
- des mesures d'aide sociale ;
- des poursuites ou sanctions pénales et administratives ;

Attention ! Une donnée n'est sensible que si elle est personnelle.

**Profil de personnalité** : La loi aborde aussi cette question. C'est l'assemblage de données permettant d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. Exemple : grand, blond, bègue, autoritaire ; le super doué de l'informatique. Sans préciser davantage, on sait de qui on parle ! Généralement, d'ailleurs, quand on entre dans la phase des propos médisants ou trop confidentiels, on supprime le nom pour en faire une simple description physique ou caractérielle : « Tu sais, machin, du département des achats qui martyrise sa secrétaire... »

**Traitement** : En fait, est considéré comme traitement, TOUTE OPÉRATION relative à des données personnelles :

- Collecte : dès qu'on questionne et qu'on cherche à obtenir des renseignements sur quel qu'un.
- Exploitation : dès qu'on travaille sur ces données – création d'un listing, marketing direct...
- Modification : ex. : toute intervention sur le fichier du personnel ; statut familial, salaires, etc.
- Communication : quand on transmet le listing des salaires à la banque pour autoriser le paiement.
- Archivage : quand on ne fait rien d'autre que de conserver des données, même aux archives. Ne rien faire, c'est faire !
- Destruction : supprimer des fichiers, constitue aussi un traitement. On ne peut pas toujours faire comme on veut. Il y a nécessité de passer au destructeur des dossiers personnels. On ne peut pas simplement virer les dossiers à la poubelle.

Sur ces différents points, les grandes caractéristiques de la LPD se résument comme suit :

- La LPD ne protège pas les données elles-mêmes.
- La LPD n'empêche pas la libre circulation de l'information, mais veille à ce que le flux s'arrête là où commence la sphère privée.
- La LPD protège le travailleur vis-à-vis de l'employeur.

### **Les grands principes applicables au traitement des données :**

Même si l'enfer est pavé de bonnes intentions, il faut remarquer que le législateur est allé assez loin dans la définition des principes applicables. On peut citer :

1. le principe de la licéité ;
2. le principe de la bonne foi ;
3. le principe de la proportionnalité ;
4. le principe de la finalité ;
5. le principe de l'exactitude des données ;
6. le principe de la sécurité des données.

*Licéité* : « Tout agissement déloyal est prohibé. » Ex. : convaincre un ex-employeur de donner des références alors que l'employé l'avait interdit, en produisant une fausse autorisation.

*Bonne foi* : La collecte ne doit pas se faire à l'insu de la personne. On doit pouvoir prévoir le traitement qui en sera fait. Ex. : document rendu insuffisamment anonyme pour faire un exemple de cours.

*Proportionnalité* : On ne doit traiter que des données qui ont un lien direct avec le but de l'opération. Ex. : dans le cadre d'un règlement de sinistre assurance, l'inspecteur ne peut pas se renseigner sur l'état d'endettement de l'assuré.

*Finalité* : On ne peut pas recueillir des données personnelles sous un faux prétexte. Ex. : sondage sur les habitudes de vacances pour faire du placement financier.

*Exactitude des données* : Quiconque traite des données personnelles doit s'assurer que celles-ci soient exactes. Ex. : une facture non payée ? client notoirement insolvable. Faux titre universitaire sur un panneau d'affichage en entreprise.

*Sécurité des données* : Les données personnelles doivent être protégées contre tout traitement non autorisé. Il faut prendre des mesures techniques pour protéger le contenu et l'organisation des données traitées.

Toutes ces dispositions impliquent de protéger les données contre : *a*) une destruction accidentelle ou non autorisée, *b*) des xxx techniques, *c*) la falsification, le vol ou l'utilisation illicite, *d*) la modification, la copie, l'accès ou autres traitements non autorisés.

Le respect des différents principes ci-dessus permet de protéger l'individu contre les autres (État, employeur, autres personnes privées), en ce qu'il est le seul maître des droits d'accès et de traitement, qu'il peut accorder à des tiers. D'où la question de savoir quels traitement sont licites.

### **3. LA LICÉITE DES CONTRÔLES**

**Principes** : Il n'est pas permis de contrôler et d'enregistrer les communications téléphoniques, les courriers électroniques et l'accès sur le Web. Il est également interdit de contrôler et d'enregistrer le comportement des individus, sauf à démontrer un intérêt prépondérant ou une obligation légale et d'avoir prévenu les intéressés.

**Contrôles les plus fréquents :**

**Le téléphone** : Le prestataire de services poursuit deux objectifs : l'établissement des communications et la facturation de ses prestations. Le fournisseur de services de télécommunications doit respecter, pour être conforme à l'art. 1 LTC, les principes suivants : *a*) de bonne foi, *b*) de proportionnalité, *c*) de finalité. La loi sur les télécommunications règle la délicate problématique du secret. L'interdiction est bien délimitée ; elle va au-delà du cercle des employés, au-delà du contenu même de la conversation et au-delà de la durée contractuelle d'emploi.

*L'usage privé du téléphone sur le lieu de travail* : Sauf interdiction absolue issue du contrat de travail, le travailleur peut utiliser le téléphone de l'entreprise dans les limites raisonnables et sans qu'aucune surveillance ne soit effectuée.

*Principe* : Les écoutes et les enregistrements des conversations privées par l'employeur sont interdites.

*Exceptions* : Dans le cas de facturation les données ne doivent pas être saisies car appartenant à la sphère privée du travailleur. Dans un but d'éviter les abus : inobservation d'une interdiction, usage disproportionné. Le contrôle préventif est interdit. Si l'usage est strictement interdit, des contrôles aléatoires sont tolérés à condition que les travailleurs en aient été prévenus et que ces contrôles se fassent sur ordre de la Direction.

*Usage professionnel du téléphone sur le lieu de travail* : Même dans le cadre professionnel, les écoutes (ou enregistrements) téléphoniques peuvent constituer une surveillance du comportement et sont de ce fait prohibées. L'écoute ou l'enregistrement d'entretiens téléphoniques professionnels est admissible sous deux conditions : *a*) la notion de sécurité, *b*) le contrôle de performance.

*Usage à des fins délictuelles* : Lorsque l'on soupçonne l'existence d'un comportement illicite, l'autorité pénale peut, sur demande de l'employeur et sans devoir en informer la personne concernée, ordonner des écoutes ou des enregistrements téléphoniques aux fins d'obtention de preuves.

*Installations* : Les caractéristiques techniques des installations modernes peuvent constituer des risques de violation de la protection des données.

**L'e-mail et Internet :**

*Axiome de base* : Le courrier envoyé, sa fréquence, les interlocuteurs contactés constituent des données qui peuvent être contrôlés par l'employeur grâce à la technique.

*Principe de droit* : l'employeur n'est pas autorisé à consulter le contenu des courriels privés.

*Le Spamming* : Envoi en masse par courrier électronique. Le Spammer peut régulièrement vous adresser un e-mail avec un virus avec l'espoir que la récurrence trompera votre attention.

*Intérêts de l'employeur* : Un ordinateur connecté à un réseau peut porter atteinte aux intérêts de l'employeur.

*Mesures de sauvegarde des intérêts de l'employeur* : a) l'employeur peut mettre en œuvre divers moyens techniques, b) établir un règlement d'utilisation, c) restreindre l'accès. En l'absence de règlement, le travailleur peut présumer que l'accès est autorisé dans le respect des principes de finalité, de proportionnalité, de bonne foi et du respect de l'art. 321 a CO.

*Les bases légales de la surveillance* : L'interdiction de procéder à une surveillance du comportement selon 26 OLT 3 n'est pas applicable de manière absolue, il faut déterminer ce qui prévaut : a) la protection de la personnalité de l'employé, b) les intérêts de l'employeur. L'employeur peut procéder à des contrôles pour vérifier la bonne application du règlement. L'employeur peut installer une surveillance personnelle s'il respecte deux conditions : a) l'information doit être préalable, b) la constatation d'un abus doit être antérieure.

*Phases de la surveillance* : Suite à la constatation des faits suspects, on peut distinguer les cas suivants : a) pas d'abus, pas de dérangement technique, b) pas d'abus, mais dérangement technique, c) abus sans dérangement technique, d) abus avec dérangement technique.

*Cas spécial du délit* : En cas de soupçons concrets suite à un contrôle anonyme, l'employeur peut sauvegarder les moyens de preuve (fichiers, journaux, sauvegardes). En cas de délit sans dérangement technique, il appartient au supérieur hiérarchique de déposer plainte. Si l'employeur continue la surveillance de son propre chef, cela peut se retourner contre lui, car seule une autorité pénale compétente peut l'ordonner.

*Cas spéciaux d'abus du courriel* : L'employeur est en droit d'identifier un collaborateur, auteur de mobbing à l'aide de courriels anonymes.

**Vidéosurveillance** : La base juridique est toujours la même (art 26 OLP 3) : « toute surveillance du comportement est interdite », même s'il s'agit d'un comportement indésirable ou illicite. En outre, il ne doit pas y avoir de contrôle à l'aide de moyens techniques. Si des systèmes de surveillance deviennent nécessaires pour d'autres raisons, il est impératif de respecter les conditions suivantes.

#### **4. VOIES DE RECOURS**

*Droit d'accès (art. 8 LPD)* : Toute personne indépendamment de son âge, de son domicile ou de sa nationalité a le droit de demander accès aux données stockées sur son compte. La procédure à suivre : a) faire une demande par écrit, b) le droit d'accès est en principe gratuit. En cas de rejet total ou partiel de la demande : c) ouverture d'une action judiciaire.

*Art. 15 LPD (Art. 25 LPD)* : « Le demandeur peut en particulier requérir que les données soient rectifiées ou détruites ou que leur communication à des tiers soit interdite. » Pour faire valoir ces prétentions, le demandeur s'adresse à la juridiction civile ordinaire (art 28 à 28 1 CC).

*Sanctions encourues* : Sanctions civiles et pénales.

Après les applaudissements de remerciements pour ce brillant exposé à deux solistes, l'assemblée termina la soirée par le traditionnel verre de l'amitié.

Jacques Maurice Chenux

Neuchâtel, le 12 avril 2003