La protection des données personnelles et les rapports de travail

La protection des données personnelles et les rapports de travail

Par Jean Meyer

INTRODUCTION

Les rapports de travail donnent lieu pour l'employeur à un traitement souvent très complet et parfois long de données personnelles relatives aux travailleurs. Etant donné leur dépendance en fait et en droit vis-à-vis de celui-là, il convient d'accorder une attention toute particulière à la protection des données personnelles et de veiller à ce que le traitement patronal de données concernant les employés ne porte pas atteinte à la personnalité de ceux-ci.

Nous aborderons tout d'abord la réglementation suisse sur la protection des données et ensuite la problématique en droit social.

A. La réglementation sur la protection des données

La loi fédérale sur la protection des données[1], qui vise à protéger la personnalité et les droits fondamentaux des personnes faisant l'objet d'un traitement de données (art. 1 Loi), a été adoptée le 19 juin 1992 par l'Assemblée fédérale de la Confédération suisse[2] et est entrée en vigueur le 1er juillet 1993[3]. Des ordonnances d'exécution, qui s'y rapportent, sont entrées en vigueur à la même date[4]. Il y a lieu de réserver également les réglementations cantonales et communales[5].

La législation suisse rattache la protection des données au droit de la personnalité[6] et non au droit de la propriété. Malgré son titre, elle ne tend pas protéger les données, mais la personnalité.

Parmi les droits fondamentaux qui sont touchés par le traitement des données personnelles figurent la liberté personnelle[7], l'autodétermination en matière d'information. Il y a aussi les aspects élémentaires à l'épanouissement de la personnalité: le libre arbitre, la liberté de prendre une décision dans des domaines essentiels pour l'épanouissement de la personnalité, la dignité, l'honneur et la sphère privée[8].

La nouvelle loi définit un certain nombre de principes pour le traitement des données qui doivent être respectés par tous les maîtres de fichiers, soumis à la loi. Elle a une fonction préventive: elle doit empêcher les manipulations potentielles et ne doit pas seulement faire le constat des déviances.

a) Champ d'application

Les dispositions légales régissent le traitement des données concernant les personnes physiques et morales[9], effectué par des personnes privées ou des organes fédéraux[10].

En revanche, elles ne sont pas applicables au traitement des données par les autorités cantonales, à moins que celles-ci ne remplissent des tâches de la Confédération par délégation, dans la mesure où il n'existe pas au niveau cantonal de prescriptions sur la protection des données.

L'article 2, alinéa 2 LPD énumère les exceptions à l'application de la loi: les dispositions légales régissant le traitement des données ne s'appliquent pas aux données personnelles qu'une personne physique traite pour son usage exclusivement personnel et qu'elle ne communique pas à des tiers, aux délibérations des Chambres fédérales et des commissions parlementaires, aux procédures pendantes civiles, pénales, d'entraide judiciaire internationale ainsi que de droit public et de droit administratif[11], aux registres publics relatifs aux rapports juridiques de droit privé, ou enfin aux données personnelles traitées par le Comité international de la Croix-Rouge.

Aux termes de l'article 3, la loi définit un certain nombre de termes, pour assurer une application uniforme de la loi:

- *données personnelles*: toutes les informations qui se rapportent à une personne identifiée ou identifiable;
- *personne concernée*: la personne physique ou morale au sujet de laquelle des données sont traitées;
- *données sensibles*: les données personnelles portant sur 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;
- *profil de la personnalité*: un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique;
- *traitement*: toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données;

– *communication*: le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant;
– *fichier*: tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée;
– *maître du fichier*: la personne privée ou l'organe fédéral qui décide du but et du contenu du fichier.

b) Dispositions générales de protection des données

A titre liminaire, on peut remarquer que la législation met en exergue six principes fondamentaux de la protection des données:
– la licéité de la collecte;
– la bonne foi dans le traitement;
– la proportionnalité du traitement;
– l'exactitude des données;
– les restrictions à la communication des données à l'étranger;
– le principe de la sécurité des données.

Toute collecte de données personnelles ne peut être entreprise que d'une manière licite; cela implique que toute collecte de données personnelles ne doit pas se faire avec des moyens trompeurs, sous la menace ou de manière dissimulée. Leur traitement doit être effectué conformément aux principes de la bonne foi[12] et de la proportionnalité[13]. Cela a notamment pour conséquence que la collecte des données doit avoir lieu auprès de la personne concernée et les données ne doivent pas être traitées contre sa volonté. En outre, le traitement des données personnelles ne doit pas être institué comme une règle, mais doit demeurer l'exception.

Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, est prévu par une loi ou ressort des circonstances (art. 4 Loi). En d'autres termes, les données à caractère personnel faisant l'objet d'un traitement automatisé sont enregistrées pour des finalités déterminées et légitimes et ne doivent pas être utilisées de façon incompatible avec ces finalités.

Il en découle que quiconque traite des données personnelles doit s'assurer qu'elles sont correctes[14]. Toute personne concernée peut requérir la rectification des données inexactes (art. 15, al 3 et 25, al 2 LPD, art. 15, al 2 OLPD).

Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une protection des données

équivalente à celle qui est garantie en Suisse. On consacre ici le principe de l'équivalence.

Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées[15]. Si la sécurité absolue n'existe pas, une absence de sécurité ou des mesures insuffisantes constituent des violations de la loi.

Le droit d'accès est garanti et est considéré à juste titre comme la clef de la protection des données[16]: ainsi, toute personne peut demander au maître d'un fichier si des données la concernant sont traitées et les contrôler; elle peut aussi voir si la législation est respectée[17]; cette maîtrise existe en tant que droit subjectif, mais aussi en tant que droit constitutionnel. De plus, il n'est pas possible de renoncer par avance au droit d'accès[18]. En exerçant son droit, la personne concernée n'a d'ailleurs aucun intérêt particulier à faire valoir. Le maître du fichier doit lui communiquer toutes les données la concernant qui sont contenues dans le fichier, le but et éventuellement la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données. Le système est construit pour protéger le maître du fichier et la personne objet du traitement.

Le maître du fichier qui fait traiter des données par un tiers demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers, s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse. Si plusieurs maîtres de fichier gèrent en commun un ou plusieurs fichiers, le droit d'accès peut être exercé auprès de chacun d'eux, à moins que l'un d'eux soit responsable de l'ensemble du traitement.

Les renseignements sont fournis dans les 30 jours suivant la réception de la requête. Si les renseignements ne peuvent être donnés dans ce délai, le maître du fichier en avertit le requérant en lui indiquant la période dans laquelle interviendra la réponse.

Ils sont, en règle générale, fournis gratuitement et par écrit, sous forme d'imprimés ou de photocopies.

Il y a, cependant, des restrictions au droit d'accès (art. 8-10 LPD[19]), aucun droit ne pouvant être exercé de manière absolue: le maître du fichier peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où une loi au sens formel[20] le prévoit, ou lorsque les intérêts prépondérants d'un tiers l'exigent (par exemple ceux d'un réfugié politique ou d'un étranger). Il peut aussi empêcher ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à des tiers. De façon générale, le maître du fichier doit indiquer le motif pour lequel il refuse de fournir, limite ou ajourne les renseignements.

Les médias bénéficient d'un régime particulier. En effet, le maître d'un fichier (en tant qu'éditeur de médias), utilisé exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique, peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où les données personnelles fournissent des indications sur les sources d'information, un droit de regard sur des projets de publication en résulte (on veut éviter une censure préventive) ou bien la libre formation de l'opinion publique est compromise[21]. Il en ressort notamment que l'exception ne s'applique ni à la partie publicitaire d'un média, ni lorsque le fichier est utilisé à des fins commerciales sous la forme de vente de données. Les journalistes peuvent, en outre, refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, lorsqu'un fichier leur sert exclusivement d'instrument de travail personnel.

La loi instaure aussi la fontion de registre, qui est public[22]. Il a pour fonction d'assurer un certain contrôle des traitements et sa tenue constitue une mesure nécessaire pour assurer l'exercice du droit d'accès. La compétence d'une telle administration incombe au préposé fédéral à la protection des données. Il procède à l'enregistrement du fichier si la déclaration est complète[23] et a été faite en bonne et due forme; auparavant, il procède à un examen sommaire de la licéité du traitement[24]. Si le maître du fichier ne déclare pas son fichier ou le fait de manière incomplète, il l'invite à s'acquitter de son obligation dans un délai déterminé; à l'expiration du délai et sur la base des informations dont il dispose, il peut procéder d'office à l'enregistrement du fichier ou recommander la cessation du traitement des données. Les organes fédéraux sont tenus de déclarer tous leurs fichiers au préposé pour enregistrement. Par contre, la loi prévoit un régime bien plus souple pour les personnes privées. Une déclaration n'est requise que pour celles qui traitent régulièrement des données sensibles ou des profils de la personnalité ou communiquent des données personnelles à des tiers; elles doivent déclarer leurs fichiers si le traitement de ces données n'est soumis à aucune obligation légale et les personnes concernées n'en ont pas connaissance; il s'ensuit que peu de dossiers devront être déclarés.

Il va de soi que les fichiers doivent être déclarés avant d'être opérationnels.

c) Traitement des données personnelles par des personnes privées

La loi précise que quiconque traite des données personnelles ne doit pas porter une atteinte illicite[25] à la personnalité des personnes concernées. Le pronom indéfini implique non seulement le maître de fichier, mais aussi ses collaborateurs ou un tiers mandaté par celui-ci. Personne

n'est en droit, sans motif justificatif, notamment de traiter des données personnelles en violation des principes définis aux articles 4, 5, alinéa 1, 6, alinéa 1 et 7, alinéa 1, ou encore de traiter des données contre la volonté expresse de la personne concernée, ou bien de communiquer à des tiers des données sensibles ou des profils de la personnalité. Il en découle qu'il est possible de repérer dix hypothèses d'atteinte énoncées par la loi sur ce plan:

- collecte illicite des données;
- traitement contraire à la bonne foi;
- traitement contraire au principe de proportionnalité;
- traitement contraire au principe de finalité;
- traitement contraire au principe de la qualité des données;
- communication indue de données à l'étranger;
- défaut de sécurité des données;
- traitement transgressant le droit d'opposition de la personne concernée;
- la communication à des tiers de données sensibles;
- la communication à des tiers de profils de la personnalité.

Pour ces cas, il y a de par la loi des fictions d'atteintes à un droit de la personnalité.

En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement. Par contre, les renseignements contenus dans les registres publics officiels ne sont pas soumis à la LPD (art 2, al 2, lit d LPD); ils sont régis par des règles spéciales en raison de leur importance pour la sécurité juridique.

L'article 13 LPD définit des motifs justificatifs, qui permettront au juge dans des litiges de pondérer les intérêts en présence. Ainsi, une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime[26], par un intérêt prépondérant privé ou public[27], ou par la loi[28]. Il y a un intérêt prépondérant si:

- le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernent le cocontractant[29];
- le traitement s'inscrit dans un rapport de concurrence économique actuel ou futur avec une autre personne, à condition toutefois qu'aucune donnée personnelle traitée ne soit communiquée à des tiers;
- les données personnelles sont traitées dans le but d'évaluer le crédit d'une autre personne, à condition toutefois qu'elles ne soient ni sensibles ni constitutives de profils de la personnalité et qu'elles ne soient communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée;

- les données personnelles sont traitées de manière professionnelle exclusivement en vue d'une publication dans la partie rédactionnelle d'un média à caractère périodique;
- les données personnelles sont traitées à des fins ne se rapportant pas à des personnes, notamment dans le cadre de la recherche, de la planification ou de la statistique, à condition toutefois que les résultats soient publiés sous une forme ne permettant pas d'identifier les personnes concernées;
- les données recueillies concernent une personnalité publique, dans la mesure où ces données se réfèrent à son activité publique[30].

Afin de consacrer la transparence nécessaire, il est requis du maître d'un fichier automatisé soumis à enregistrement (art. 11, al 3 LPD) d'élaborer un règlement de traitement décrivant en particulier l'organisation interne et les procédures de traitement et de contrôle des données[31] et comprenant les documents relatifs à la planification, à l'élaboration et à la gestion du fichier et des moyens informatiques.

Le traitement de données personnelles peut être confié à un tiers aux conditions suivantes:

- le mandant veille à ce que ne soient pas effectués des traitements autres que ceux qu'il est lui-même en droit d'effectuer;
- aucune obligation légale ou contractuelle de garder le secret ne l'interdit;
- le tiers peut faire valoir les mêmes motifs justificatifs que le mandant.

En édictant des sanctions civiles, le législateur fédéral a choisi en principe de renvoyer aux actions judiciaires du code civil suisse, tout en y ajoutant des règles spécifiques à la protection des données en raison du domaine[32]. Les articles 28 à 28l CCS régissent les actions et les mesures provisionnelles concernant la protection de la personnalité. Le demandeur[33] peut en particulier requérir que les données soient rectifiées ou détruites ou que leur communication à des tiers soit interdite. Si ni l'exactitude, ni l'inexactitude d'une donnée personnelle ne peut être établie, il peut requérir que l'on ajoute à la donnée la mention de son caractère litigieux. Il peut demander que la rectification ou la destruction des données, l'interdiction de la communication, la mention du caractère litigieux ou le jugement soient communiqués à des tiers ou publiés. Les actions en exécution du droit d'accès peuvent être ouvertes au domicile du demandeur ou à celui du défendeur. Le juge statue selon une procédure simple et rapide. Mais pas gratuite!

B. Le préposé fédéral à la protection des données

L'individu seul n'est pas en mesure de faire face à la complexité du traitement des données. Il fallait donc instituer un organe de surveillance spécialisé et indépendant. Le législateur a adopté cette solution, ce qui est innovateur dans le droit suisse.

Le préposé fédéral à la protection des données est nommé par le Conseil fédéral. Il s'acquitte de ses tâches de manière autonome[34] et est rattaché administrativement au Département fédéral de justice et police[35]. Il dispose d'un secrétariat permanent.

Sa mission consiste dans les tâches suivantes:

- il surveille l'application par les organes fédéraux de la loi fédérale sur la protection des données et des autres dispositions fédérales relatives à la protection des données. Aucune surveillance ne peut être exercée sur le Conseil fédéral;
- il assiste les organes fédéraux et cantonaux dans le domaine de la protection des données;
- il se prononce sur les projets d'actes législatifs fédéraux et de mesures fédérales qui touchent de manière importante à la protection des données[36];
- il collabore avec les autorités chargées de la protection des données en Suisse[37] et à l'étranger;
- il examine dans quelle mesure la protection des données assurée à l'étranger est équivalente à celle que connaît la Suisse;
- il établit les faits d'office ou à la demande de tiers; lorsqu'en application des articles 27 et 29 LPD, le préposé fédéral est amené à éclaircir les faits, notamment pour apprécier la licéité d'un traitement, il peut demander au maître du fichier des informations relatives notamment:
  a) aux mesures techniques et organisationnelles prises ou envisagées (art. 8 à 10, 20 OLPD);
  b) aux règles relatives à la rectification, au blocage, à l'anonymisation, à la sauvegarde, à la conservation et à la destruction des données;
  c) à la configuration des moyens informatiques;
  d) aux connexions de fichiers;
  e) au mode de communication des données;
  f) à la description des champs de données et des unités d'organisation qui y ont accès;
  g) à la nature et à l'étendue de l'accès des utilisateurs au fichier.
- il conseille les personnes privées en matière de protection des données[38];

Exemple:

Un grand nombre d'entreprises offrent la possibilité à leurs collaborateurs de garer leurs véhicules sur des places de parking appartenant à l'entreprise ou louées à l'extérieur à cet effet. Les collaborateurs reçoivent à cette fin une vignette de parcage sous forme de carton à placer sur le tableau de bord ou d'étiquette à coller à l'intérieur du pare-brise. Selon le préposé, l'utilisation de vignettes autocollantes peut donc être considérée comme proportionnelle. Il n'est pas nécessaire pour le contrôle des véhicules garés que les vignettes contiennent des indications en langage clair sur l'employeur. Une marque neutre ou une combinaison de lettres et de chiffres intelligibles uniquement par la personne chargée du contrôle suffit donc amplement à assurer le but du contrôle.

– il fait rapport au Conseil fédéral à intervalles réguliers et selon les besoins[39].

Dans le secteur privé[40], le préposé établit les faits d'office ou à la demande de tiers lorsque une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système), des fichiers doivent être enregistrés, ou des communications à l'étranger doivent être déclarées. Il peut exiger la production de pièces, demander des renseignements et se faire présenter des traitements. Le droit de refuser de témoigner au sens prévu par l'article 16 de la loi fédérale sur la procédure administrative s'applique par analogie. Après avoir établi les faits, le préposé à la protection des données peut recommander de modifier ou de cesser le traitement. Si une telle recommandation du préposé est rejetée ou n'est pas suivie d'effet, il peut porter l'affaire devant la Commission fédérale de la protection des données pour décision, qui est une commission d'arbitrage et de recours au sens des articles 71a à 71c de la loi fédérale sur la procédure administrative.

On relèvera que les décisions de la Commission peuvent être contestées, par la voie du recours de droit administratif, devant le Tribunal fédéral.

C. La protection des données personnelles dans le monde du travail

La protection des données dans les rapports de travail revêt un aspect majeur de la problématique du traitement des données par des personnes privées.

Un nouvel article 328b CO est entré en vigueur en même temps que la loi sur la protection des données[41]. Il est ainsi libellé: «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».

Cette disposition est une norme spéciale établissant, dans le domaine de la législation sur le contrat de travail, une protection des données spécifique à propos du traitement, par l'employeur, de données personnelles concernant le travailleur. Elle concrétise les principes généraux du traitement des données, notamment le principe de la proportionnalité. En effet, elle prévoit que l'employeur est autorisé à traiter des données relatives aux travailleurs dans deux cas seulement et uniquement dans une mesure précise: dans le cadre de la conclusion d'un contrat de travail, il est autorisé à traiter des données concernant les candidats afin de déterminer s'ils sont aptes à remplir l'emploi en question; par ailleurs, durant les rapports de travail, il peut traiter les données nécessaires à l'exécution du contrat de travail.

Dans la pratique, il se pose différents problèmes:

a) Procédure d'engagement:

Les problèmes relatifs à la protection des données surgissent dès la publication d'une offre d'emploi. Il arrive qu'une telle offre soit publiée sous chiffre, sans indication de l'employeur ou de l'organisme recruteur. Or, si les candidats ne connaissent pas l'identité de l'annonceur, ils ne peuvent faire valoir leur droit d'accès. Il peut en découler des difficultés lorsqu'on veut savoir si le dossier de candidature a été conservé ou non. En vertu de la loi, le maître d'un fichier qui charge un tiers de traiter des données demeure tenu de fournir les renseignements demandés. Cette obligation incombe, toutefois, au tiers s'il ne révèle pas l'identité du maître du fichier. Il s'ensuit que l'éditeur du journal ou l'entreprise de recrutement de personnel doivent donner l'identité de l'annonceur au candidat «malheureux» pour qu'il puisse exercer son droit d'accès.

Concernant les candidatures, l'employeur ne peut demander que des documents ou poser des questions qui se rapportent aux qualités requises par l'emploi en question et dont il a besoin objectivement pour faire son choix. En principe, le travailleur possède un droit à l'autodétermination sur ses données personnelles. Il en va de même de la recherche de renseignements auprès de tiers sur les candidats. **Par exemple, on ne peut demander de renseignements auprès de l'employeur précédent que si la personne a donné son accord**. De plus, les informations essentielles recueillies ne peuvent porter que sur les prestations et le comportement du travailleur[42]. Il est notamment illicite de garantir l'accès au dossier du travailleur, ou de communiquer les conditions du contrat de travail, car la position du candidat pourrait s'en trouver considérablement affaiblie.

L'analyse graphologique de l'écriture d'un candidat n'est également autorisée qu'avec l'accord exprès de celui-ci. Ce genre d'analyse répond en général à la définition du profil de la personnalité (assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique) et contient souvent des indications révélatrices sur la personne en question. L'usage qui consiste à demander à tous les candidats une lettre de candidature manuscrite pour le cas échéant faire établir une analyse graphologique n'est pas conforme aux exigences de la loi sur la protection des données.

Utiliser un seul questionnaire médical pour deux finalités différentes (aptitude à l'emploi et admission dans la caisse de pensions) est contraire aux principes de proportionnalité et de finalité de la LPD.

Quant à un service médical d'une entreprise lors du recrutement, il n'est autorisé à communiquer par un rapport que ses conclusions quant à la capacité, respectivement le degré et la durée d'incapacité de travail de la personne concernée.

Il ressort en outre de l'article 328b CO et du principe de la proportionnalité que les dossiers des candidats qui n'ont pas été retenus doivent leur être retournés et que les éventuelles copies doivent être détruites immédiatement après conclusion de la procédure d'engagement. Les expertises graphologiques et les tests suivent le même sort.

b) Durant les rapports de travail:

Durant les rapports de travail, l'employeur tient un dossier personnel concernant le travailleur. Conformément à l'article 328 CO, il ne doit contenir que les données nécessaires à l'exécution du contrat de travail.

Faut-il informer le préposé à la protection de la tenue de ce type de dossiers?

S'ils ne contiennent que des données dont le traitement par l'employeur est soumis à une obligation légale, si la personne concernée en a connaissance ou s'il n'y a pas de traitement régulier de données sensibles ou de profils de la personnalité, ni communication régulière de données à des tiers, ces fichiers ne sont pas soumis au devoir d'annonce. Inversement, il y a un devoir de déclaration.

Il ressort de l'article 8 LPD que toute personne employée dispose d'un droit d'accès complet au contenu de son dossier[43]. Le travailleur doit par conséquent pouvoir contrôler quels éléments de sa vie privée et de son itinéraire dans l'entreprise figurent dans son dossier. Ce droit d'accès ne peut être limité qu'exceptionnellement et dans des cas fondés. Il n'est notamment pas admis de limiter systématiquement la consultation des qualifications. Les dossiers du personnel doivent être tenus de manière à ce que l'on puisse renseigner les travailleurs sur tout et à ce que le droit d'accès ne soit qu'exceptionnellement limité. Par exemple, il est permis de restreindre ce droit d'accès afin de protéger des intérêts

prépondérants de tiers (p. ex en cachant le nom de l'auteur d'une analyse graphologique). L'expertise graphologique peut être conservée comme pièce du dossier personnel, mais ne devrait pas être librement accessible à l'intérieur du dossier.

Les données doivent en général être communiquées par écrit, sous forme d'imprimé ou de photocopie. En accord avec l'employeur ou sur sa proposition, la personne concernée peut également consulter ses données sur place. Mais dans ce cas également, elle doit avoir la possibilité de demander des copies.

Si l'employeur n'autorise pas un travailleur à consulter son dossier ou refuse de lui en communiquer le contenu, quels sont les moyens de défense du travailleur?

Il peut saisir le juge qui ordonne l'accès au dossier (art. 15, al 4 LPD).

Si lors de la consultation, il constate que des renseignements sont inexacts ou portent atteinte à sa personnalité, il peut requérir du juge, en cas de refus patronal, que ces données soient rectifiées, sinon détruites ou pour le moins que leur communication à de futurs employeurs ou à des tiers soit interdite (art. 15 LPD). Pour le cas où l'employeur méconnaît une telle injonction et cause de ce fait une atteinte particulièrement grave à la personnalité du travailleur, celui-ci est en droit de demander une indemnité pour tort moral (art. 49 CO).

Les actions judiciaires dans ce contexte relèvent de la juridiction du travail.

Des employeurs utilisent ou envisagent d'introduire, à des fins d'évaluation périodique, des tests[44] informatisés d'aptitude. En raison des risques pour la protection de la personnalité que représente le recours à de tels produits, il est impératif que leur utilisation soit la plus stricte possible. Les exigences suivantes doivent être remplies:

- le respect des principes généraux tels ceux de la finalité et de la proportionnalité des données, la fiabilité et l'objectivité des résultats;
- il faut examiner quelles conceptions de l'être humain ou de la personnalité sont à la base de la méthode de test adoptée; celle-ci ne doit pas être choisie sans regard critique; il convient d'examiner quelle méthode de test correspond le mieux à la culture de l'entreprise et à la fonction à examiner;
- par principe, il convient de garder une attitude critique vis-à-vis des résultats des tests; ceux qui sont isolés doivent être mis en rapport avec l'ensemble de la personnalité et des capacités de la personne testée;
- le caractère facultatif de la participation aux tests doit être assuré et ne doit pas entraîner des désavantages ouverts ou déguisés;
- l'application des méthodes de test doit être précédée d'une analyse précise des performances requises; les résultats du test doivent don-

ner des informations parlantes en rapport avec les performances des collaborateurs examinés;
- le professionnalisme de la conduite des tests et de leur analyse doit être assuré;
- l'original des résultats du test doit être remis à la personne testée après achèvement de la procédure, et les autres documents (copies comprises) doivent être détruits;
- la compréhensibilité des données par l'employé doit être assurée;
- la personne testée doit dans tous les cas avoir la possibilité de se prononcer personnellement sur les résultats du test et leur interprétation;
- les tests ne doivent pas être utilisés comme moyen unique ou principal de gestion des ressources humaines; ils ne remplacent en aucun cas l'entretien personnel d'évaluation, de sélection ou de promotion;
- l'anonymisation des tests dont les résultats sont envoyés à des experts externes ou au concepteur du test pour évaluation, respectivement amélioration de la qualité du produit, doit être garantie.

Dans le contexte de la qualification des travailleurs (mais aussi de l'établissement de certificats intermédiaires et de certificats de départ), se pose la question de savoir si les opinions sur le travailleur constituent des données personnelles et s'il existe un droit à la rectification (art. 5, al 2 LPD) de ces opinions. Dans la mesure où elles sont ou peuvent être mises en relation avec une personne identifiée ou identifiable, les opinions constituent des données personnelles. Ces opinions doivent être contrôlées quant à leur exactitude et si nécessaire rectifiées.

L'employeur ne peut tenir une liste des adresses privées des collaborateurs et en permettre l'accès aux autres collaborateurs que si elle est nécessaire aux activités professionnelles. Par exemple, tel est le cas lorsque des employés doivent être régulièrement contactés à leur domicile. Lorsqu'il suffit que le central téléphonique puisse atteindre les employés à leur domicile, l'employeur ne doit la remettre qu'à ce service.

Du point de vue des règles générales de la protection de la personnalité, nul n'est habilité à consulter l'agenda[45] d'une personne, et encore moins à en faire des photocopies, ni à exiger la destruction de certaines pages. Le détenteur dudit agenda est au demeurant libre d'y annoter ce que bon lui semble, puisqu'il lui est propre [46].

La communication des motifs détaillés d'absence en cas de maladie (médecin, cure, maladie, convalescence, thérapie) dans un programme hebdomadaire qui n'est pas seulement accessible à l'entourage professionnel immédiat de la personne concernée, mais à un grand nombre de personnes, n'est pas conforme aux prescriptions de la protection des données; cela peut effectivement avoir pour conséquence une atteinte à la personnalité de la personne concernée. Conformément au principe de

la proportionnalité, les données sur la santé des employés ne peuvent être relevées par l'employeur que dans la mesure où elles sont nécessaires au bon déroulement des rapports de travail (notamment poursuite du versement du salaire et établissement du plan de travail pendant une absence pour cause de maladie). De même, ces données ne peuvent être communiquées par l'employeur à l'intérieur de l'entreprise qu'aux personnes qui en ont besoin du fait de leur activité (service du personnel, supérieurs et collaborateurs directs de la personne concernée). Pour les autres, il suffit en général d'une communication précisant que la personne intéressée est absente durant une période déterminée. Pour cette raison, il est conseillé de n'indiquer que les absences dues à un motif professionnel, et d'inscrire les absences pour d'autres motifs (maladie, vacances, congés, etc.) sous une dénomination unique.

Enfin, se pose la question de savoir dans quelle mesure l'employeur peut communiquer des données concernant les employés à des tiers:

- L'employeur peut à coup sûr communiquer des données pour remplir une obligation prévue par la loi. Dans d'autres cas, la communication de données personnelles à des tiers peut se transformer aisément en violation de la personnalité et doit être pratiquée avec prudence, vu le devoir d'assistance qu'a l'employeur envers le travailleur.
- La pratique largement répandue consistant à octroyer à des tiers (par ex., bailleurs, organismes délivrant des cartes de crédit) des renseignements sur le revenu d'un travailleur sans obligation légale est contestable. Ce genre de renseignements devraient être recueillis par les tiers directement auprès de la personne concernée. Dans tous les cas, l'employeur ne doit les communiquer qu'avec l'accord du travailleur.

c) Après la fin des rapports de travail:

à ce stade-là, une question se pose à tout employeur: que va-t-il faire des données dont il dispose sur son ex-employé?

Après l'achèvement du rapport de travail, l'employeur n'est en droit de conserver que les données dont il a besoin pour la dissolution du rapport de travail et pour l'accomplissement d'éventuelles obligations post-contractuelles[47] (par ex. établissement du certificat ou comptabilité, obligations relevant du droit des assurances sociales) (art. 328b CO). Toutes les autres données traitées doivent être détruites. C'est le cas des expertises graphologiques et des tests d'aptitude.

La protection contre les atteintes aux droits de la personnalité au sens des articles 28ss CCS est imprescriptible. En tant que règles spéciales d'application de cette norme, l'article 328b CO et la LPD suivent le même sort. La protection s'étend aussi bien pendant, qu'après la fin des rapports de travail, sans limitation dans le temps.

d) Autres

Sur un autre plan, l'utilisation de systèmes de surveillance et de contrôle des travailleurs au poste de travail est aussi une question épineuse. Que faut-il entendre sous ce terme ?

Sont considérés comme systèmes de surveillance et de contrôle tous les dispositifs techniques[48] qui permettent d'observer, séparément ou par groupes, les activités ou le comportement des employés. En font notamment partie les appareils pour le relevé électronique des compteurs électriques. Ne serait-ce que pour des raisons de protection de la santé, l'employeur n'a pas le droit d'utiliser de tels systèmes s'ils sont destinés à surveiller le comportement des travailleurs à leur poste de travail (art. 26 de l'ordonnance 3 relative à la loi sur le travail). L'utilisation de systèmes de surveillance et de contrôle est par contre autorisée pour des raisons de sécurité et pour calculer le rendement (p. ex. enregistrement du nombre de frappes par jour dans un système d'élaboration de textes). Néanmoins, l'employeur ne peut utiliser de tels systèmes qu'après en avoir préalablement informé les employés concernés.

L'enregistrement de données téléphoniques ne saurait avoir pour but de contrôler le comportement des employés. Le relevé des numéros d'abonnés dont le raccordement a été appelé pour des raisons professionnelles est admissible dans la mesure où il est effectué non pas pour contrôler le comportement des employés, mais bien pour des motifs d'ordre professionnel (p. ex. en vue de facturer la communication au client), et pour autant que les employés en soient informés. Un relevé des numéros d'abonnés à des raccordements privés que les employés composent (ou dont ils reçoivent des appels) ne doit en aucun cas être établi lorsque les conversations téléphoniques privées ne sont pas interdites d'une manière générale. Les indicatifs locaux peuvent, le cas échéant, être enregistrés. L'interdiction de tenir des conversations privées doit être imposée par des moyens autres que la surveillance des communications téléphoniques, par exemple en imposant l'établissement des communications externes via une centrale ou en ne permettant qu'à certains raccordements d'établir des communications directes. Lorsque le numéro d'appel s'affiche automatiquement, il convient de veiller à ce que l'affichage puisse, au besoin, être déconnecté par les deux correspondants. La transmission d'un appel à un raccordement autre que celui qui a été sélectionné doit être signalée à temps, de façon à ce que l'auteur de l'appel puisse interrompre la liaison. Le contenu de conversations téléphoniques ne peut être enregistré qu'à des fins de contrôle de performances (par ex. vente par téléphone ou objectifs didactiques) ou pour des motifs de sécurité. Cette mesure de contrôle éminemment incisive n'est admissible que si la personne dont la conversation est enregistrée ou écoutée y consent, et pour autant qu'elle en soit chaque fois informée à temps et de manière claire (par ex. par le biais d'un signal optique ou acoustique).

Le rappel pour contrôle des abonnés appelés est inadmissible dans tous les cas. De même, l'écoute de conversations entre employés (par ex. par le biais d'un interphone équipé à cet effet) n'est en aucun cas autorisée. Lorsqu'une telle interdiction est en vigueur, les employés doivent avoir la possibilité, en cas d'urgence ou durant les pauses, de téléphoner depuis un raccordement non surveillé.

En cas de recours à des systèmes de surveillance pour des raisons de sécurité, il convient de veiller à ce que le dispositif choisi ménage autant que possible les employés. Si par exemple, dans un grand magasin, une surveillance contre le vol est assurée par le biais de caméras vidéo, il convient d'éviter dans toute la mesure du possible que leur champ n'englobe les employés. Cette règle vaut également pour les installations de guidage de la production. Lorsqu'une surveillance des personnes elles-mêmes est nécessaire pour des raisons de sécurité (par ex. pour être en mesure d'intervenir lors de situations dangereuses), il convient d'examiner des solutions de rechange (par ex. réponse à un message transmis à espaces réguliers, faute de quoi l'alarme se déclenche).

Une affaire judiciaire concernant ce type de problèmes a eu pour cadre le Jura.

Ainsi, la FTMH a ouvert action contre une entreprise en demandant le démontage ou la mise hors service d'une installation de surveillance par vidéo des ateliers. La Cour civile du Tribunal cantonal a limité dans la procédure les débats à la question de la qualité pour agir de la demanderesse. Elle a résolu cette question par la négative. L'atteinte à la personnalité des travailleurs que le syndicat alléguait, contre tout bon sens, n'aurait pas été suffisamment grave pour qu'il puisse se prévaloir d'un intérêt collectif dépassant les intérêts individuels de ses membres. La demanderesse a recouru en réforme sur ce point et a obtenu gain de cause, avec raison, auprès du Tribunal fédéral.

Selon la Haute Cour, la qualité pour agir des associations professionnelles est subordonnée à la condition qu'elles soient habilitées par leurs statuts à sauvegarder les intérêts économiques de leurs membres et que ceux-ci aient eux-mêmes qualité pour intenter l'action (ATF 86 II 21, c. 2, JdT 1960 I 583s; ATF 73 II 65, JdT 1948 I 11). Elles peuvent ester en justice pour défendre les intérêts communs d'une profession dépassant l'intérêt personnel de leurs membres (ATF 86 II 23, JdT 1960 I 584), notamment lorsqu'il y va de la protection de la personnalité des travailleurs.

En l'occurrence, la cour cantonale n'avait pas à se demander, à ce stade de la procédure, si l'installation litigieuse constituait une atteinte aux droits de la personnalité des travailleurs, le cas échéant, si cette atteinte était grave. Elle ne devait se soucier que de la réalisation, dans le cas d'espèce, des conditions jurisprudentielles sus-rappelées. Or, ces conditions étaient ici remplies. En particulier, l'atteinte aux droits de la per-

sonnalité des travailleurs invoquée par la demanderesse pour le démontage ou la mise hors service de l'installation litigieuse dépassait l'intérêt personnel de ses membres et touchait tout individu exerçant un semblable métier (ATF 114 II 64, FTMH c. Saner, 8 novembre 1988).

Dans un arrêt du 19 septembre 1989 (RJJ 1991, p.60ss), la Cour civile du canton du Jura a admis, au vu des faits, qu'une caméra vidéo ayant pour champ les ateliers ou bien étant orientée sur une machine automatique, qui permet de contrôler le travailleur occupant l'emplacement de celle-ci, constituait une atteinte à la personnalité des employés. Il en va de même si la caméra n'est pas enclenchée. Il a été ordonné sa mise hors service.

A l'instar du secteur de la santé, le domaine des assurances requiert le traitement de données sensibles et de profils de la personnalité. Il est doté de normes matérielles spécifiques de protection des données. D'autre part, lorsque la LPD s'applique, elle pose un certain nombre de problèmes aux caisses de pension et aux caisses professionnelles en particulier, telle la question de l'annonce des fichiers au préposé.

Ainsi, si une caisse cantonale de compensation gère des fichiers de données personnelles en application du droit cantonal, par exemple en matière d'allocations familiales, elle les annonce aux autorités cantonales de protection des données dans les cantons dotés d'une telle loi.

Lorsqu'une telle caisse exécute du droit fédéral (AVS, par exemple), elle les déclare également. Les autorités cantonales de protection des données sont compétentes. Dans les cantons qui ne disposent pas encore d'une telle législation, l'annonce est faite auprès de l'organe de contrôle cantonal que ces cantons sont quand même tenus de désigner selon la LPD.

Quant à la caisse professionnelle qui agit en tant que personne privée (par exemple, pour le traitement des prestations des conventions collectives – fonds de vacances, etc.), elle est uniquement soumise au devoir d'annonce dans les cas prévus par la LPD. Pour les fichiers qu'elle gère en tant qu'organe fédéral (prévoyance professionnelle obligatoire LPP), elle est toujours soumise au devoir d'annonce, comme tous les organes fédéraux et ce pour les motifs suivants:

- ces institutions accomplissent une tâche fédérale;
- le deuxième pilier relève du domaine des assurances sociales, ce que le Conseil fédéral a confirmé dans son avis du 17 avril 1991 intitulé «Initiative parlementaire, droit des assurances sociales», concernant en particulier le projet de loi fédérale sur la partie générale du droit des assurances sociales;
- l'affiliation à une institution est obligatoire;
- les contestations entre institutions de prévoyance, employeurs et ayants-droit ne sont pas réglées selon la procédure civile, mais selon la procédure administrative. En effet, au niveau fédéral, la voie

du recours de droit administratif au Tribunal fédéral des assurances est ouverte;
- si l'on se réfère à l'ordonnance du Conseil fédéral sur la création de la fondation fonds de garantie LPP, les subsides versés aux institutions de prévoyance sont assimilables à des subventions.

Un article 50, alinéa bis LAVS est entré en vigueur le 1er janvier 1995, simultanément à la loi fédérale sur l'impôt fédéral direct. Il a trait à l'obligation des organes de l'AVS de renseigner les autorités fiscales. Il supprime l'obligation de garder le secret des organes de l'AVS à l'endroit des autorités chargées de l'exécution des lois fiscales. Sur la base de cette disposition, la Conférence des fonctionnaires fiscaux d'Etat avait demandé à recevoir systématiquement certaines informations. Le préposé fédéral à la protection des données a été consulté à plusieurs reprises sur l'étendue de l'obligation d'entraide incombant aux organes de l'AVS. Il est parvenu à la conclusion selon laquelle le caractère obligatoire mis à part, cette norme s'inscrit dans la ligne des principes généraux de l'entraide administrative, que l'on peut résumer en ces termes:
- une base légale doit prévoir expressément la communication d'informations;
- une demande motivée est déposée dans un cas d'espèce;
- les renseignements sont nécessaires à la législation fiscale;
- les informations n'ont pas pu être collectées auprès du contribuable ou de son employeur.

Une caisse de pension ne peut infliger une réserve à un nouvel assuré, qui refuse de répondre à un questionnaire ad hoc, mentionnant la question suivante: «avez-vous effectué un test-SIDA au résultat positif?». En effet, cette question est disproportionnée. Les connaissances scientifiques en matière d'incidences de la séropositivité sur l'évolution de la santé sont insuffisantes pour justifier la focalisation sur le SIDA plutôt que sur d'autres maladies, telle la malaria. De ce fait, il n'est pas justifié d'infliger systématiquement une réserve de cinq ans aux personnes ayant répondu par l'affirmative à cette question, ainsi qu'à celles ayant refusé d'y répondre.

Dans un arrêt 1P.478/1995 du 9 mai 1996, le Tribunal fédéral a précisé que les informations sur la prévoyance professionnelle d'un prévenu sont secrètes. Le secret auquel est tenu une caisse de pensions doit être opposé au juge pénal. Les faits étaient les suivants: une procédure pénale avait été ouverte en Argovie pour trafic de drogue contre un ressortissant de l'ex-Yougoslavie. Dans le but d'assurer le paiement des frais de la procédure et d'une éventuelle amende, le ministère public avait tenté de faire bloquer l'avoir de libre passage dont l'intéressé disposait auprès de sa caisse de prévoyance professionnelle. La caisse et l'assuré avaient recouru contre cette décision auprès du Tribunal cantonal en se prévalant de l'insaisissabilité des fonds de prévoyance professionnelle. Ils avaient

obtenu gain de cause, mais en partie seulement: la saisie était refusée, mais la caisse s'était vu imposer d'informer le juge si son affilié faisait une demande de paiement en vue d'un départ de Suisse. Cette dernière décision a été cassée par la Haute Cour, toujours sur recours de la caisse et de l'assuré. Insaisissable aujourd'hui, l'avoir de libre passage de ce dernier pourra être confisqué pour payer ses frais de justice au moment où lui-même en disposera. Tel sera notamment le cas s'il quitte la Suisse et fait à ce moment-là une demande de paiement. Le juge ne peut, toutefois, pas exiger de la caisse qu'elle le renseigne sur le moment où ce versement interviendra. Les caisses de prévoyance, en effet, sont tenues au secret sur la situation personnelle et financière de leurs affiliés. Une ordonnance du Conseil fédéral énumère exhaustivement les personnes et les autorités à l'égard desquelles ce secret peut être levé. Le juge pénal n'en fait pas partie et le renseignement exigé fait incontestablement partie de ceux couverts par le secret.

CONCLUSIONS

La technique influence fortement l'organisation du travail. Poussée à l'extrême, elle peut provoquer des dysfonctionnements et des problèmes humains.

Les conditions de travail sont aujourd'hui difficiles en raison de la conjoncture et des mutations technologiques. Il n'est pas toujours facile de faire valoir ses droits lorsqu'on est sur le qui-vive à son poste de travail. Cependant, issue des droits de l'homme, la protection des données personnelles est un excellent moyen de défense pour faire respecter sa personnalité et sa dignité de travailleur. C'est également un état d'esprit. Pour l'employeur, c'est un aspect important de la gestion des ressources humaines. De manière générale, les partenaires sociaux ont un rôle essentiel à jouer pour sa concrétisation réelle dans le monde du travail.

Transgresser épisodiquement ou à de nombreuses reprises cette protection conduit assez rapidement à la résurgence moderne de formes insidieuses d'esclavage.

Jean Meyer (Nyon) est chef du personnel et juriste.

NOTES

[1]BELSER U.: *«Das Recht auf Auskunft, die Transparenz der Datenbearbeitung und das Auskunftsverfahren»*, in: SCHWEIZER R.J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zürich 1993, S. 55-65. CLUSIS: *«Protection des données, Que faire pour être en règle avec la*

loi sur la protection des données?», Ed. CLUSIS, Lausanne 1994. GILLARD N. (Ed.): *«La nouvelle loi fédérale sur la protection des données»*, Ed. CEDIDAC, Lausanne 1994. MUELLER P.: *«Die Grundzüge des Entwurfs für ein schweizerisches Datenschutzgesetz, insbesondere im Vergleich mit den Regelungen einiger Nachbarstaaten»*, in: ZBl 89/1988, Nr 10, S. 425-437. NABHOLZ L.: *«Entstehung und Grundanliegen des Datenschutzgesetzes»*, in: SCHWEIZER R. J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zürich 1993, S. 1-7. PEDRAZZINI M. M.: *«Der Ausbau des Datenschutzes»*, in: Festchrift für Bundesrat Kurt Furgler, Zürich/Köln 1984, S. 316-324. PEDRAZZINI M.M.: *«Die Grundlagen des Datenschutzes im Privatbereich: die Grundzüge und der Geltungsbereich des Bundesgesetzes»*, in: SCHWEIZER R.J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zürich 1993, S. 81-90. PETER J. TH.: *«Das Datenschutzgesetz im Privatbereich, Unter besonderer Berücksichtigung seiner motivationalen Grundlage»*, Dissertation Zürich 1994. SAUTER R.M.: *«Die institutionalisierte Kontrolle im Bundesgesetz über den Datenschutz vom 19. Juni 1992, Eine rechtsvergleichende Analyse»*, Schulthess Polygraphischer Verlag, Zürich 1995.

[2]FF 1988 II 421ss; RO 1993, 1945ss; RS 235.1.

[3]ACF du 14 juin 1993 (RO 1993, 1959).

[4]Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD). Ordonnance du 14 juin 1993 concernant le traitement des données personnelles lors de l'application de mesures préventives dans le domaine de la protection de l'Etat. Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale (OALSP).

[5]BELSER U.: *«Kontrolle des Datenschutzes in Kantonen und Gemeinden: Konzepte, Erfahrungen und Empfehlungen»*, in: SCHWEIZER R.J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zürich 1993, S. 107-120. SCHWEIZER R. J./B. LEHMANN: *«Datenschutzrecht/ Droit de la protection des données»*, Ed. Schulthess, Zurich 1993. SCHWEIZER R. J.: *«Die Verwirklichung des Datenschutzes in der öffentlichen Verwaltung»*, in: HANGARTNER Y./SCHWEIZER R.J. (Hrsg): Aktuelle Fragen des Datenschutzes in Kantonen und Gemeinden, St-Gallen 1990, S. 21-47.

[6]Avec ses éléments de droit public sauvegardant la liberté personnelle comme droit fondamental (ATF 113 Ia 257) et ses éléments de droit privé (art. 28 CCS). Voir aussi: SALADIN P.: *«Persönliche Freiheit als soziales Grundrecht?»*, in: Mélanges A. BERENSTEIN, Lausanne 1989, p. 89-114. TERCIER P.: «Le nouveau droit de la personnalité», Ed. Schulthess, Zurich 1984.

[7]DRUEY J.N.: *«Persönlichkeit als Postulat oder als Objekt des Rechtsschutzes»*, in: RDS 95/1976 I p. 377ss. HALLER W.: *«La liberté personnelle»*, in: Commentaire de la Constitution fédérale de la Confédération suisse, Bâle/Zurich/Berne 1993. ROSSINELLI M.: *«Les libertés non écrites»*, Ed. Payot, Lausanne 1987, p. 127ss. SALADIN P.: *«Persönliche Freiheit als soziales Grundrecht?»*, in: Mélanges A. BERENSTEIN, Ed. Payot, Lausanne 1989, p. 89ss. Voir aussi: ATF 90 I 29; 111 Ia 231.

[8]MUELLER J. P: *«Die Grundrechte der Verfassung und der Persönlichkeitsschutz des Privatrechts»*, Thèse Berne 1964.

TERCIER P.: *«Le nouveau droit de la personnalité»*, Ed. Schulthess, Zurich 1984, p. 17ss.

[9]L'extension aux personnes morales est conditionnée par l'article 53 CCS.

[10]On entend, par organe fédéral, l'autorité ou le service fédéral ainsi que la personne en tant qu'elle est chargée d'une tâche de la Confédération (art. 3, let h LPD). Cela vise aussi les personnes physiques et morales qui exécutent des tâches publiques pour le compte de la Confédération: p. ex. SUVA, caisses de compensation privées, ou encore caisses maladies.

[11]A l'exception des procédures administratives de première instance.

[12]Selon KNAPP B. (*«Précis de droit administratif»*, Ed. Helbing & Lichtenhahn, Bâle 1991, p. 105), le principe de la bonne foi peut se définir de la manière suivante: «Il nous paraît qu'en droit public le principe de la bonne foi doit être subdivisé en plusieurs sous-principes. On distinguera ainsi: le principe de la bonne foi proprement dit, selon lequel l'Etat et l'administré doivent s'en tenir à leurs déclarations et ne doivent pas chercher à se tromper par des manifes-

tations de volonté inexactes ou incomplètes; le principe de la confiance selon lequel l'Etat doit respecter la sécurité juridique et l'administré n'est tenu de faire quelque chose ou n'en est dispensé que dans la mesure où il pouvait ou devait le comprendre; l'interdiction de l'abus de droit, qui empêche l'administré d'utiliser son pouvoir ou son droit à des fins pour lesquelles il n'est pas destiné». Voir aussi: MOOR P.: *«Droit administratif»*, Vol I, Ed. Staempfli, Berne 1988, p. 358ss. PICOT F.: *«La bonne foi en droit suisse»*, in: RDS 1977 II p. 116ss. WEBER-DUERLER B.: *«Vertrauensschutz öffentlichen Recht»*, Bâle 1983.

[13]D'après KNAPP B. (op. cit., p. 113), «la jurisprudence (ATF 102 Ia 522 X; 97 I 508 Griessen) définit le principe de la proportionnalité de deux manières: selon la formule sommaire, il signifie que la mesure prise doit permettre d'atteindre le but qu'elle recherche. Selon la formule plus élaborée, la mesure prise doit être propre à atteindre le but recherché tout en respectant le plus possible la liberté de l'individu, d'une part, et un rapport raisonnable doit exister entre le résultat recherché et les limites à la liberté nécessaires pour atteindre ce résultat, d'autre part». Voir aussi: HUBER H.: *«Ueber den Grundsatz der Verhältnismässigkeit im Verwaltungsrecht»*, in: RDS 1977 I p. 1ss. MOOR P.: *«Droit administratif»*, Vol I. Ed. Staempfli, Berne 1988, p. 350ss. MUELLER P.: *«Le principe de la proportionnalité»*, in: RDS 1978 II p. 197ss. ZIMMERLI U.: *«Der Grundsatz der Verhältnismässigkeit im öffentlichen Recht, Versuch einer Standortbestimmung»*, in: RDS 1978 II p. 1ss.

[14]Le principe doit être relativisé: FF 1988 II 458. WALTER J. PH.: *«Le droit public matériel»*, in: La nouvelle loi fédérale sur la protection des données, Ed. Cedidac, Lausanne 1994, p. 51s.

[15]Voir notamment les art. 8-12 et 20 OLPD.

Voir sur le plan plus technique: CERSSI: *«Sécurité et qualité informatiques, Nouvelles orientations»*, Ed. Presses polytechniques et universitaires romandes, Lausanne 1995. LAMERE J.M./ROSE P./TOURLY J.: *«Protection des systèmes d'information; qualité et sécurité informatiques»*, Ed. Dunod, Paris 1992. LAMERE J.M.: *«Sécurité des systèmes d'information»*, Ed. Dunod, Paris 1991.

[16]PAGE G.: *«Le droit d'accès aux données personnelles: fondements, étendue, limites»*, in: La nouvelle loi fédérale sur la protection des données, op. cit., p. 113ss. PAGE G.: *«Le droit d'accès et de contestation dans le traitement des données personnelles»*, Zurich 1982. MAURER U.: *«Ausgewählte Datenschutzrechtliche Ansprüche»*, in: Der Schweizer Treuhänder 4/1994, S. 245-250.

[17]Afin de sauvegarder ses intérêts personnels, la personne concernée peut faire valoir son droit sous la forme d'une action de droit privé (art. 15 LPD), d'un recours administratif (art. 25 LPD) ou d'un recours de droit administratif, ou encore de plainte au préposé fédéral (art. 27 LPD). Des sanctions pénales sont prévues: art. 34 et 35 LPD et art. 179 novies et 321bis CPS.

[18]Voir aussi art. 28 CCS.

[19]Voir aussi les art. 14 et 15 OLPD.

[20]On entend, par loi au sens formel: les lois fédérales et arrêtés fédéraux de portée générale sujets au référendum, les résolutions d'organisations internationales contraignantes pour la Suisse et les traités de droit international approuvés par l'Assemblée fédérale, comportant des règles de droit.

[21]PEDRAZZINI M.M.: *«Privatrechtliche Schranken der Medienfreiheit»*, in: Mélanges A. KOLLER, Berne 1993, p. 407ss.

[22]Il peut être consulté gratuitement. Une liste des fichiers enregistrés est publiée périodiquement dans la Feuille fédérale.

[23]Voir art. 3, 16 et 17 OLPD. Exceptions à la publication: art. 4, 18 OLPD.

[24]Lorsque le fichier à enregistrer viole des prescriptions sur la protection des données, le préposé fédéral recommande de modifier, de cesser ou de ne pas entreprendre le traitement. Il suspend l'enregistrement jusqu'à la régulation de la situation.

[25]STEINAUER P.H.: *«Le droit privé matériel»*, in: La nouvelle loi fédérale sur la protection des données, op. cit., p. 86ss. STEINAUER P.H.: *«Die Verletzung durch private Datenbearbeitung und die allfällige Rechtfertigung einer Verletzung: Einzelheiten der gesetzlichen*

Regelung», in: SCHWEIZER R.J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zurich 1993, p.. 43-53.

[26]Le consentement de la personne concernée n'est soumis à aucune forme particulière; la LPD renvoie à l'art. 11 CO. Il peut être exprès ou tacite, mais de par la LPD il doit en tout cas être éclairé. De plus, la personne peut révoquer son consentement en tout temps. Un engagement indéterminé à ce propos est contraire au droit de la personnalité et de la LPD par conséquent.

[27]Voir ATF 97 II 97 = JdT 1972 I 242.

[28]Voir notamment art. 52 CO.

[29]FF 1988 II 466ss.

[30]ATF 71 II 191 = JdT 1945 I 566; ATF 52 I 263 = JdT 1927 I 22; ATF 111 II 209 = JdT 1927 I 22.

[31]Le maître du fichier indique au destinataire l'actualité et la fiabilité des données personnelles qu'il communique, dans la mesure où ces informations ne ressortent pas des données elles-mêmes ou des circonstances.

[32]PIOTET D.: *«Les actions civiles: un premier bilan»*, in: La nouvelle loi fédérale sur la protection des données, op. cit., p. 143ss.

[33]PEDRAZZINI M.M.: *«Der Rechtschutz der betroffenen Personen gegenüber privaten Bearbeitern (Klagen, vorsorgliche Massnahmen, Gerichtsstand)»*, in: SCHWEIZER R.J. (Hrsg): Das neue Datenschutzgesetz des Bundes, Zürich 1993, p. 81-90.

[34]Il agit, à sa guise, intervenant soit à la demande de particuliers ou d'autorités fédérales, soit de sa propre initiative. De plus, il demeure libre d'agir ou non (FF 1988 II 485).

[35]Voir l'art. 31 OLPD.

[36]Voir l'art. 32 OLPD.

[37]Le préposé conseille la Commission d'experts du secret professionnel en matière de recherche médicale (art. 321bis CPS). Si cette commission a autorisé la levée du secret professionnel, il surveille le respect des charges qui grèvent l'autorisation. A cet effet, il peut établir les faits au sens de l'article 27, alinéa 2 de la loi fédérale sur la protection des données. Il peut porter les décisions de la commission d'experts devant la Commission fédérale de la protection des données. Il fait en sorte que les patients soient informés de leurs droits.

[38]Les avis (art. 28 LPD) du préposé fédéral sont soumis à émolument; l'ordonnance du 30 octobre 1985 instituant des émoluments pour les prestations de l'Office fédéral de la justice est applicable. Cette solution est pour le moins peu adaptée. En revanche, aucun émolument ne peut être prélevé auprès des autorités fédérales ou cantonales (art. 33, al 2 OLPD).

[39]Les rapports périodiques sont publiés. Désormais, ces rapports sont payants, à commander à l'Office fédéral du matériel et des imprimés, ce qui est pour le moins peu opportun au niveau de la connaissance de cette institution.

S'il en va de l'intérêt général, il peut informer le public de ses constatations et de ses recommandations. Il ne peut porter à la connaissance du public des données soumises au secret de fonction qu'avec le consentement de l'autorité compétente. Si celle-ci ne donne pas son consentement, le président de la Commission fédérale de la protection des données tranche; sa décision est définitive.

[40]SCHWEIZER R.J.: *«Die Aufsicht über die privaten Datenarbeitungen und die Beschwerdemöglichkeiten privater Bearbeiter undbetroffenen Personen gegen Aufsichtsentscheide»*, in: Das neue Datenschutzgesetz des Bundes, Zurich 1993, p. 96ss.

[41]Message du Conseil fédéral concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988 (FF 1988 II 421ss).

[42]Il va de soi que l'employeur potentiel n'est pas en droit de recueillir sur le travailleur des renseignements que, selon la loi, il ne pourrait pas obtenir de ce dernier personnellement.

[43]ATF 120 II 118 = JdT 1995 I 141 (arrêt rendu sous l'ancien droit).

[44]G. AZZOPARDI: Mesurez votre Q. I, Ed. Guide Marabout, Alleur 1989. G. AZZOPARDI: Réussir les tests d'entreprise pour triompher dans la course à l'emploi, Ed. Marabout, Al-

leur 1983. E. RAUDSEPP: Etes-vous créatif, Ed. Albin Michel, Paris 1983. J.J. LARANE: La pratique des tests psycho-techniques, Ed. L'écrit, Paris 1992.

[45]Un agenda ne constitue par un fichier au sens de la LPD, du moment qu'il n'est pas structuré de manière à retrouver les informations par personne concernée.

[46]Pour qu'il y ait usage exclusivement personnel, il faut que les informations ne soient pas utilisées hors du cercle restreint de la vie personnelle, ce qui implique notamment qu'elles ne soient pas communiquées à des collègues de travail.

[47]En règle générale, on recommande une durée de conservation de 5 ans, qui exceptionnellement peut être prolongée à 10 ans, par exemple, lorsque la loi le prévoit.

[48]Font partie des systèmes de surveillance et de contrôle:

- les centraux téléphoniques. Même de petits centraux téléphoniques, dont le coût n'est pas très élevé, permettent aujourd'hui d'enregistrer et d'établir le relevé des appels qui entrent et qui sortent, y compris les numéros des abonnés, ainsi que la durée et le prix de chaque communication. Souvent aussi, il est très aisé d'écouter les conversations téléphoniques à l'insu des personnes concernées;
- les systèmes TED. Les systèmes de traitement électronique des données sont eux aussi dotés de nombreuses possibilités de surveillance et de contrôle. Au moyen de moniteurs intégrés au matériel ou au logiciel, il est par exemple possible d'enregistrer: le moment auquel un ordinateur est utilisé, si des configurations sont modifiées, les programmes qui sont actionnés ou déconnectés, les activités exécutées au sein d'un programme déterminé. Les messages transmis par courrier électronique peuvent généralement être ouverts et lus sans difficultés.
- les autres systèmes. Il convient de relever que d'autres systèmes, qui n'ont pas pour objectif premier de surveiller le personnel, peuvent être utilisés à cette fin (par ex. lorsqu'ils sont équipés d'un code d'accès électronique et d'un compteur automatique). Tel est par exemple le cas des photocopieurs, des fax, des systèmes d'enregistrement du temps, des systèmes de déroulement des travaux, des contrôles d'accès, des compteurs, etc.