11ème Rapport d'activités 2003/2004

Préposé fédéral à la protection des données

Rapport d'activités 2003/2004 du Préposé fédéral à la protection des données

Le Préposé fédéral à la protection des données est tenu de fournir périodiquement au Conseil fédéral un rapport sur son activité (article 30 de la loi fédérale sur la protection des données). Le présent rapport couvre la période du 1er avril 2003 au 31 mars 2004.

Ce rapport est également disponible sur Internet (www.edsb.ch)

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

La protection des données est en pleine mutation. Dans le monde occidental, la peur face au terrorisme qui, selon toute apparence, fera dorénavant partie de notre quotidien, met à l'épreuve les principes démocratiques. Nul ne contestera que le terrorisme est un fléau et que nous devons y parer grâce à la coopération internationale et à une meilleure information. Par contre, un certain flou règne sur ce qui est autorisé, dans une démocratie, au titre de la prévention. Le but essentiel d'une mesure préventive est d'isoler les stratégies terroristes dans leur contexte social. Une prévention ainsi définie devrait en premier lieu viser à assurer les droits humains élémentaires - y compris les droits sociaux et économiques - à cette frange de la population susceptible de servir de soutien et de vecteur au terrorisme. Tant que les mesures antiterroristes ne pourront empêcher que les activistes mis hors d'état d'agir ne soient aussitôt remplacés par de nouvelles cellules terroristes, la prévention n'aura pas atteint son but.

Hélas, le débat actuel montre que l'objectif premier de la prévention est l'arrestation des éventuels coupables par des moyens policiers. Ainsi, il est question d'écoutes téléphoniques préventives ou de mesures d'écoute dans les locaux privés hors de toute procédure pénale. Avant tout examen de la constitutionnalité de ces écoutes, nous devons souligner que cette stratégie ne saurait être payante, également à long terme, que si elle permet d'éradiquer le terrorisme. Mais sur ce point, les doutes sont plus que permis.

Une discussion intéressante sur les aspects fondamentaux de ce genre de mesures a eu lieu dernièrement en Allemagne. Au printemps 2004, le Tribunal constitutionnel fédéral a restreint massivement les possibilités de mettre en place des écoutes téléphoniques et accru considérablement la protection des espaces privés. La pratique en matière d'écoutes était contraire à la dignité humaine et, de ce fait, largement anticonstitutionnelle. Selon l'arrêt rendu par ce tribunal, la surveillance acoustique d'appartements et de conversations téléphoniques demeurent en principe possible, mais doit être accompagnée de conditions nettement plus strictes. Outre le fait que le «cœur de la sphère privée» doit toujours être respecté, le Tribunal constitutionnel requiert concrètement que ce genre de méthodes de surveillance n'entre en considération qu'en cas de délits graves. Ces principes sont tout à fait applicables à la Suisse car nous disposons de bases constitutionnelles comparables en matière de droits fondamentaux.

La question est d'actualité dans notre pays aussi. En effet, on parle depuis peu de permettre des écoutes téléphoniques en dehors de toute procédure pénale. Terrain délicat s'il en est, dont le point le plus discutable est le fait qu'une telle surveillance - puisqu'elle pourrait être ordonnée indépendamment de l'introduction d'une procédure pénale - ne prendrait pas place dans le cadre d'une procédure conforme aux principes de l'Etat de droit et qu'il n'y serait pas obligatoirement mis un terme par l'arrêt de la procédure pénale ou par la levée de l'accusation. Actuellement, la personne surveillée a la possibilité de consulter elle-même les dossiers et peut au plus tard à ce stade contrôler la légalité de la mesure appliquée. La surveillance préventive sans procédure pénale sonnerait le glas de cette possibilité de contrôle.

Du reste, il convient de souligner qu'avant de créer de nouvelles lois, on ne doit pas uniquement s'interroger sur l'efficacité des mesures mises en discussion, mais en tout premier lieu examiner l'efficacité des lois existantes. En temps de crise, le législateur a trop souvent tendance à réagir par la création de nouvelles lois avant d'analyser si les lacunes proviennent de l'absence de lois adéquates ou uniquement de l'application de celles qui existent déjà.

A l'échelon international aussi, diverses mesures sont débattues et arrêtées. En mars de cette année, l'Union européenne a adopté une volumineuse déclaration de lutte contre le terrorisme. Parmi les mesures étudiées, plusieurs ne servent pas la lutte antiterroriste. Pour chaque mesure envisagée, il est indispensable de se demander si elle est nécessaire et adaptée à la lutte contre le terrorisme ou bien si elle sert plutôt à imposer une large surveillance de la population et un contrôle social et politique. Il est évident qu'un rapport tendu lie le respect des droits de l'homme et la garantie de la sécurité publique C'est la raison pour laquelle il faut peser attentivement les intérêts en jeu. Il est permis de douter que cette pesée des intérêts en jeu soit suffisamment respectée. Même s'il est compréhensible et nécessaire que les Européens soient d'une très grande fermeté face aux forces terroristes violentes, il est indispensable qu'un Etat de droit veille attentivement aux intérêts en jeu et examine les mesures préconisées à la lumière de leur nécessité, de leur utilité et de la proportionnalité.

Comme on a pu le lire dernièrement dans un article de la presse dominicale, d'aucuns viennent même de découvrir les mesures de surveillance et les préconisent au titre de moteur de la croissance économique. Il va de soi que considérée dans cette perspective, la protection des données n'est plus qu'un «corset» dont il faut se défaire. On rêve donc de pouvoir exploiter du point de vue économique aussi les «possibilités de liaison par le biais des réseaux de surveillance électroniques». Rien d'étonnant à cela lorsque l'on sait que dans ce genre de structure de pensée très axée sur l'économie de marché, le fait que la protection de la sphère privée a une dimension constitutionnelle est totalement ignoré et n'est même pas mentionné dans le cadre d'une appro-

che mettant en balance sécurité publique, efficacité économique et droits individuels garantis par la Constitution. Il est par ailleurs occulté qu'une protection des données efficace est justement essentielle au fonctionnement d'une économie fondée sur la concurrence.

Si l'on préconise la mise en place de réseaux de surveillance électronique, il convient aussi de souligner que les possibilités techniques actuelles permettent des contrôles comme ceux décrits par G. Orwell. Le marquage par puce électronique (les étiquettes RFID, technique d'identification utilisant la communication par radio) permet de localiser les biens, les personnes ou leurs services sur tout le territoire. Les informations recueillies pourraient aisément être mises en relation avec d'autres banques de données (données concernant les communications téléphoniques, achats par carte de crédit, comptes en banque, cartes-clients, etc.) permettant des profils de la personnalité forts détaillés. Depuis longtemps, l'homme transparent n'est plus une métaphore littéraire, mais une possibilité à portée de main.

Ce sont là des perspectives d'avenir qui préoccupent les Suisses, comme nous l'a montré un sondage représentatif publié au printemps 2004 à propos du nouveau Conseil suisse pour la protection de la personnalité, un «lobby mis sur pied pour défendre les droits de la personnalité au sens large». Bien qu'une majorité écrasante des personnes interrogées ait accordé une priorité absolue à la protection de la personnalité, une tout aussi grande majorité est persuadée que l'on ne peut guère se protéger contre l'utilisation abusive des données et que les lois actuelles ne suffisent pas. Il s'agit là d'une invitation claire faite au législateur d'accorder la priorité à la protection de la personnalité, étant donné les menaces qui grandiront encore du fait du progrès technique, et d'améliorer les instruments législatifs à cet effet.

Hanspeter Thür

Répertoire des abréviations

AG	Assemblée générale
ATF	Arrêts du Tribunal fédéral
CA	Conseil d'administration
CFPD	Commission fédérale de la protection des données
CIRCA	Communication & Information Resource Centre Administrator
Cst.	Constitution fédérale
DDPS	Département fédéral de la défense, de la protection de la population et des sports
FF	Feuille fédérale
IDA	Interexange of Data between Adminisrations (échange d'informations entre administrations publiques)
LAA	Loi fédérale sur l'assurance-accidents
LAMal	Loi fédérale sur l'assurance-maladie
LCA	Loi fédérale sur le contrat d'assurances
LPD	Loi fédérale sur la protection des données
LSA	Loi fédérale sur la surveillance des assurances
OFAS	Office fédéral des assurances sociales
PFPD	Préposé fédéral à la protection des données
RFID	Radio Frequency Identification
SA	Société anonyme
SUVA	Caisse nationale Suisse d'assurance en cas d'accidents
WPISP	Groupe de travail sur la sécurité de l'information et la protection de la sphère privée de l'OCDE
ZIS	Système central d'information

1. Droits fondamentaux

1.1 Thèmes divers

1.1.1 Loi sur les publications officielles: risques et problèmes attachés à la publication de données personnelles sur Internet

Nous avons été invités, dans le cadre de la consultation des offices concernant la loi sur les publications officielles, à nous prononcer sur les risques et problèmes inhérents à la publication de données personnelles sur Internet par un organe fédéral. Les données personnelles ainsi publiées peuvent être appelées par le biais de moteurs de recherche électronique dans le monde entier et surtout sans limite de temps. Avant de publier des données sur les citoyens, un organe fédéral doit se livrer à des réflexions approfondies car l'Etat justement a un devoir particulier de respecter le droit constitutionnel de chaque personne à la protection de ses données personnelles contre un usage abusif.

La loi sur les publications officielles réglemente la publication des recueils du droit fédéral et de la Feuille fédérale. La Feuille fédérale contient la publication, entre autres, de noms de personnes qui font l'objet de notifications, décisions ou citations.

Le projet de révision prévoit notamment que les données personnelles publiées sous forme électroniques (donc également via Internet) doivent être rendues anonymes et qu'une publication de données personnelles sur Internet doit demeurer l'exception. Selon le projet de révision, cette possibilité doit être expressément prévue dans une loi spécifique. Nous avons soutenu cette solution quant à la publication de données personnelles sur Internet par un organe fédéral.

Base légales

La Constitution fédérale garantit à chaque personne la protection de ses données personnelles contre un usage abusif. Selon la définition de la LPD, on entend par données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable. La LPD ne fait donc pas la distinction entre données positives et données négatives, mais les protège sans jugement dans leur globalité. La LPD prévoit une qualification spécifique pour les données sensibles et les profils de la personnalité.

Conformément à la LPD, un organe fédéral n'est en droit de traiter des données personnelles que s'il existe une base légale à cet effet. L'accès à des données sensibles ou à des profils de la personnalité par le biais d'une procédure d'appel (par exemple sur Internet) doit être expressément prévu par une loi au sens formel.

La norme légale doit répondre de manière suffisamment précise aux exigences suivantes:

- définition du but du traitement
- détermination, dans les grandes lignes, du volume du traitement de données (les personnes concernées doivent pouvoir s'en faire une idée),
- détermination des personnes participant au traitement des données (personnes traitant les données et destinataires des données),
- mention des catégories de données traitées (dans la mesure où des données sensibles ou des profils de la personnalité sont concernés).

Problème de la publication de données personnelles sur Internet

Les informations publiées dans la Feuille fédérale peuvent être mises en relation avec des données figurant dans d'autres registres publics et des fichiers privés accessibles au public. Cela peut tout à fait concerner des données personnelles sensibles. Toutes les informations accessibles peuvent même parfois permettre d'établir des profils de la personnalité.

Il existe de nombreuses entreprises qui se sont spécialisées dans la collecte et l'exploitation systématique de données personnelles. Dans ce but, elles utilisent entre autres des informations extraites des publications officielles (feuilles officielles, registres du commerce, registres des faillites, etc.) et établissent à partir de là des fichiers (par ex. fichiers de données sur la solvabilité, fichiers d'adresses ou fichiers relatifs au monitoring [surveillance systématique et continue]).

La pratique montre que dans ce cas, les données personnelles peuvent être stockées des années durant (par ex. sur des listes d'archives des exploitants de moteurs de recherche) et ne sont plus contrôlées quant à leur actualité ou leur exactitude. Dans bien des cas, les personnes concernées n'ont pas connaissance du stockage ou du traitement de données personnelles les concernant. L'exercice de leurs droits (droit d'accès, droit de rectification, droit de destruction des données conformément à la LPD) n'en est que plus difficile. La publication de données personnelles sur Internet se traduit immanquablement pour les personnes concernées par la perte totale de la maîtrise sur leurs propres données.

Il ne faut pas en sous-estimer les répercussions pour les personnes concernées: des tiers peuvent rassembler et diffuser sans contrôle les informations collectées (par ex. solvabilité, appréciation du comportement en matière d'achats, poursuites et sanctions des autorités). Il est fort probable qu'à l'avenir, toutes les données personnelles publiées par une autorité sous forme électronique (par ex. données du registre foncier ou informations sur les personnes dont les noms sont publiés dans la Feuille fédérale), sont relevées de manière ciblée et connectées avec d'autres données avant d'être exploitées. Les personnes traitant ces données peuvent être non seulement des particuliers, mais aussi des autorités suisses et étrangères.

Après la publication, le service officiel, en tant que responsable proprement dit des données, perd toute influence sur l'utilisation ultérieure des données personnelles par des tiers. Les personnes concernées doivent donc s'attendre à ce que des données à l'origine accessibles au public soient encore utilisées par des tiers - sans possibilités d'influence ou de contrôle - dans un autre but que le but initial. C'est justement la publication de données personnelles sur Internet qui accroît considérablement le risque d'abus. La protection des données ne peut être assurée du fait même des particularités d'Internet (manque de garantie quant à la confidentialité, intégrité et authenticité des données personnelles).

Les risques principaux attachés à la publication de données personnelles sur Internet sont les suivants:

- Les informations publiées sont accessibles dans le monde entier, notamment dans des Etats qui ne sont pas dotés d'une législation équivalente à la législation suisse sur la protection des données.
- La recherche de ces informations (aussi et surtout les noms) peut se faire à partir de tous les pays du monde.
- Du fait de cette publication, non seulement les personnes directement concernées, mais aussi la personne responsable qui a traité le fichier à l'origine perdent effectivement tout contrôle sur les traitements ultérieurs.
- Certaines informations peuvent être comprises de manière totalement différente par rapport au sens qu'elles avaient à l'origine. Cela peut s'exprimer en premier lieu par un malentendu découlant des circonstances entourant une situation imprévue. D'autre part, il est possible que certaines personnes ou organisations utilisent les informations dans un but auquel nul n'avait pensé lors de leur publication et poursuivent ainsi des fins contraires à celles des personnes concernées.

- Les informations publiées ne peuvent pratiquement plus être détruites. Ce qui est publié échappe ensuite à tout contrôle.
- Il n'est jamais totalement exclu que des données soient modifiées par hasard ou intentionnellement, se transformant ainsi en données inexactes.
- Les données sont maintenues en ligne plus longtemps que le but envisagé ne le nécessite.

Analyse

Le droit fondamental visant la protection de la sphère privée (art. 13, al. 2 Cst.) oblige l'Etat à protéger ses citoyens de l'emploi abusif des données qui les concernent. Confrontée à la question de savoir si les publications officielles de données personnelles doivent, à l'avenir aussi, avoir lieu sur Internet, l'autorité responsable doit prendre en compte tous les risques. Cela implique aussi que l'autorité ne néglige pas les répercussions possibles d'un traitement de données sur Internet dont elle est à l'origine.

L'art. 13 Cst. pose aux autorités des limites claires quant à la communication électronique de données personnelles. En raison des risques inhérents à cette communication, un organisme étatique doit *en principe* s'abstenir de publier sur Internet des données personnelles de citoyens.

Le problème essentiel n'est donc pas de savoir si les répercussions de la publication d'un nom ou de l'information qui l'accompagne menacent la personnalité du citoyen concerné ou si son contenu est ressenti comme positif ou négatif par la société. Même l'affirmation selon laquelle la simple publication d'un nom n'est pas vraiment si grave ne tient pas.

Le point important est de veiller à *la manière* dont ces informations peuvent être par la suite utilisées. Aujourd'hui, les moyens de communication permettent un traitement complet et incontrôlable des données personnelles, traitement qui n'a plus rien à voir avec l'objectif premier des publications officielles. En d'autres termes: une publication (officielle) peut avoir des répercussions négatives pour une personne des années après, bien qu'à l'époque, le but initial de la publication ait semblé judicieux ou ait été licite.

Une autorité doit veiller à ce que la manière dont les données personnelles sont traitées ne porte *à aucun moment* atteinte à la personnalité de celui qui est concerné.

Le droit fondamental à la protection de la sphère privée, le principe de la proportionnalité et le principe de finalité, ainsi que l'art. 19, al. 3 LPD n'autorisent qu'une seule possibilité: les organes étatiques sont tenus de rendre anonymes les données per-

sonnelles publiées sous forme électronique. Les exceptions ne sont possibles que lorsque conformément à une base légale formelle, un certain but de traitement requiert la publication de données personnelles déterminées.

Tribunal fédéral

A propos de la publication de certains arrêts du Tribunal fédéral sur Internet, se reporter à notre 9ème Rapport d'activités 2001/2002, paragraphe 2.3.3

(http://www.edsb.ch/f/doku/jahresberichte/tb9/kap3c.htm#233).

A propos de la position du criminel dans la vie publique et du droit à l'oubli, se reporter à l'ATF 109 II 353ss..

1.1.2 Transfert de données personnelles par les compagnies aériennes aux autorités américaines

La communication de données personnelles concernant les passagers par les compagnies aériennes suisses aux autorités américaines basée sur un accord entre la Suisse et les Etats-Unis est la meilleure solution au regard des exigences de la législation sur la protection des données. La solution de l'information des passagers ne résout pas tous les aspects de protection des données dès lors que d'une part le consentement des personnes concernées ne peut être qualifié de libre et que d'autre part les données sont transmises dans un Etat ne disposant pas d'une protection des données équivalente à celle qui est garantie en Suisse. Cependant, cette solution pourrait être appliquée dans l'attente de l'entrée en vigueur d'un accord bilatéral.

Dans le domaine de la lutte contre le terrorisme, les autorités américaines, en plus de nombreuses mesures de sécurité supplémentaires, exigent des compagnies aériennes desservant les Etats-Unis (départ, arrivée et transit) un accès à l'ensemble des données concernant les passagers. En cas de refus, les sanctions peuvent aller jusqu'à l'interdiction d'atterrir sur le territoire américain. Pour pouvoir communiquer des données personnelles aux autorités américaines, les compagnies aériennes suisses, en tant que personnes privées, doivent disposer d'un motif justificatif: une disposition légale, un intérêt prépondérant public ou privé ou encore le consentement des personnes concernées.

Les lois américaines ne sont pas applicables en Suisse et il n'existe à l'heure actuelle aucun traité entre les Etats-Unis et la Suisse prévoyant la communication systématique de toutes les données concernant les passagers se rendant sur le territoire américain, venant de ce pays ou transitant par celui-ci.

Les mesures prévues par les autorités américaines ne répondant pas au principes de proportionnalité et de finalité, un intérêt public ou privé prépondérant ne peut être invoquer. En effet, la collecte de nombreuses données personnelles, y compris des données sensibles sur la santé ou celles permettant de révéler la religion, n'est pas proportionnelle. Les finalités mentionnées par les autorités américaines sont beaucoup trop vagues et ne se limitent pas à la lutte contre le terrorisme. Les durées de conservation prévues sont bien trop longues. Les ressortissants non américains n'ont aucune possibilité concrète de faire valoir leurs droits en cas d'abus lors de l'utilisation de leurs données personnelles par les autorités américaines.

La solution restante est celle d'informer les personnes concernées et de requérir leur consentement. En outre, les Etats-Unis ne disposant pas d'une protection des données équivalente à celle qui est garantie en Suisse, la question de la protection des données communiquées doit être réglée par le biais d'un contrat avec les autorités américaines. Ce contrat doit mentionner notamment le but de la communication, la durée de conservation, les règles sur l'effacement et préciser que les données ne seront pas utilisées à d'autres fins. De plus, dans le respect du principe de finalité, seules les données des personnes souhaitant actuellement voyager vers les Etats-Unis devraient être communiquées aux autorités américaines. Une telle solution n'est pourtant pas satisfaisante. D'une part, le consentement des personnes concernées ne peut être qualifié de libre. D'autre part, un contrat réglementant les traitements de données tel que susmentionné ne pourra apporter de garantie absolue face à l'utilisation des données dans le cadre de mesures législatives américaines particulières. Une autre voie que celle mentionnée ci-dessus consiste en l'élaboration d'un accord avec les autorités américaines donnant un cadre légal à ces communications de données.

Les autorités suisses, à l'instar des autorités européennes, ont décidé d'engager des négociations avec les autorités américaines. Sous la direction de l'Office fédéral de l'aviation civile, un groupe de travail interdépartemental, auquel nous participons, a pour tâche d'élaborer un accord permettant d'assurer les liaisons aériennes avec les Etats-Unis tout en respectant les principes généraux de protection des données. En attendant la mise en place d'un tel accord et à fin d'une part de ne pas pénaliser les voyageurs et d'autre part d'assurer une protection minimale de leurs données personnelles, il serait envisageable d'appliquer, à titre provisoire, la solution consistant à informer les passagers et à requérir leur consentement.

Voir également paragraphe 11.4.1.

1.2 Cyberadministration

1.2.1 Travaux concernant les questions de protection des données liées à la cyberadministration

En relation avec ce que l'on appelle la cyberadministration, il existe dans l'administration un grand nombre de projets d'envergure, ce qui empêche le PFPD de les suivre sérieusement. Pour cette raison, nous avons signalé aux responsables de différents projets que, dans leur organisation de projet, ils doivent aussi définir les responsabilités en matière de protection des données et acquérir le savoir-faire requis.

Comme déjà mentionné dans les deux précédents rapports d'activités, les objectifs des différents projets dans le domaine de l'administration électronique sont formulés de manière extrêmement vague. Par exemple, l'annexe 2 de la stratégie de la Confédération en matière de cyberadministration (état avril 2003), décrit l'objectif du Guichet Virtuel comme la simplification de la prise de contact avec les autorités, la transparence accrue des activités des autorités et la réalisation de transactions. De telles formulations d'objectifs ne permettent pas de mener des réflexions significatives sur la protection et la sécurité des données, car des objectifs clairs constituent une condition impérative pour de telles réflexions. En ceci nous nous voyons confronté à une contradiction conceptuelle insoluble. Nous sommes en outre confrontés à la situation problématique où aussi bien le nombre des projets que leur envergure nous mettent dans l'impossibilité de les suivre ne serait-ce qu'approximativement. Pour rapprocher ces deux problèmes d'une solution, nous avons rendu les responsables des projets attentifs à ce qui devrait constituer une évidence: étant donné que les mandants de projets de cyberadministration sont responsables du respect de la protection des donnés dans leurs projets, ils doivent aussi veiller à définir les responsabilités appropriées dans l'organisation de projet. Les responsables des projets doivent également s'assurer que le savoir-faire en matière de protection des données existe dans le cadre de leurs projets.

2. Protection des données – questions d'ordre général

2.1 Protection et sécurité des données

2.1.1 EDSB-Office: système de gestion des affaires à haute confidentialité et disponibilité des données.

En complément à l'actuelle haute confidentialité assurée par le chiffrement des données «sensibles» réalisé dans le cadre d'une infrastructure à clés publiques, la récente migration de notre système sur deux serveurs en grappe a permis d'offrir une haute disponibilité de nos données. La redondance des serveurs permet en outre de conduire les indispensables opérations de maintenance pendant les heures normales de travail et surtout sans rupture de service.

Fruit d'un développement répondant aux exigences internes élevées en matière de confidentialité des données (cf. notre 8ème Rapport d'activités 2000/2001 paragraphe 7.5), EDSB-Office a continué d'évoluer tant du point de vue des fonctionnalités que de la disponibilité des données. Pour mémoire, on peut simplement rappeler que la confidentialité est obtenue par chiffrement et déchiffrement sur chaque poste de travail de toutes les données «sensibles» manipulées, y compris les mandats d'impression vers les imprimantes du réseau. Il va de soi que ces mesures techniques vont de pair avec des mesures organisationnelles équivalentes, de façon à atteindre globalement le niveau de confidentialité visé. Fondée sur une classique base de données relationnelles, notre application nécessite la mise sur pied d'une infrastructure à clés publiques (PKI: Public Key Infrastructure) basée en l'occurrence sur le logiciel PGP (Pretty Good Privacy). La génération de la paire de clés, la gestion physique de la clé privée protégée par «passphrase», ainsi que l'importation des clés publiques utiles, a permis à chaque utilisateur d'acquérir une expérience pratique de la cryptographie asymétrique. Ces éléments sont néanmoins complètement intégrés dans l'application, si bien que l'utilisateur peut se concentrer sur son travail quotidien, soit la gestion de documents, dossiers et échéances, dans un environnement bureautique absolument standard. Les différents groupes de chiffrement assurent une lisibilité différenciée des documents, ce qui permet de respecter le principe de proportionnalité, qui implique également de ne pas octroyer tous les droits de déchiffrement aux administrateurs de l'application. La faisabilité d'un stockage des données «sensibles» sous forme chiffrée est ainsi démontrée, tant du point de vue sécuritaire, qu'économique et opérationnel. Les temps de réponse lors de l'enregistrement ou l'ouverture de documents sont tout à fait satisfaisants dans un environnement matériel parfaitement conventionnel.

S'agissant des fonctionnalités, on relèvera tout d'abord la recherche en plein texte permettant de retrouver n'importe quel document enregistré, sur la base de quelques mots clé significatifs de son contenu. On mentionnera ensuite l'interface bidirectionnelle avec la messagerie Outlook, qui offre l'avantage essentiel d'une parfaite intégration des courriels entrants ou sortants dans le système de gestion des affaires, évitant ainsi l'écueil de l'archivage parallèle de ces informations dont l'importance va croissant.

Enfin, on remarquera que la disponibilité des données a été fortement accrue en 2003 grâce à la mise en service de serveurs en grappe («clusterisés»). Les services de fichiers, de bases de données et d'impression sont ainsi intégralement disponibles moins d'une minute après une interruption de serveur. Cette aptitude peut d'ailleurs être exploitée pour réaliser les indispensables opérations de maintenance technique pendant les heures normales de travail et sans rupture de service. La machine en état de veille est actualisée pendant la marche de la machine en service, sur laquelle la même actualisation peut avoir lieu, après une reprise intégrale du service par la machine actualisée durant la veille. Une haute intégrité des données étant offerte par le logiciel et le matériel actuels, EDSB-Office peut ainsi être qualifiée d'application offrant une sécurité intégrale (confidentialité, intégrité, disponibilité) des données.

2.1.2 Normes en matière de sécurité et protection de l'information

Parmi les nombreux standards portant sur la sécurité de l'information, notre attention s'est portée sur le standard international ISO 17799 qui constitue un référentiel très complet en la matière. Son dernier volet couvre notamment la conformité légale, en particulier les aspects de protection des données. Le standard BS7799-2 permet ensuite une transition naturelle vers le domaine de l'audit, qui fait par ailleurs l'objet d'un nouvel article proposé dans le cadre de la révision de notre loi sur la protection des données.

La sécurité de l'information relève des aspects aussi bien technologiques que juridiques de la sécurité et protection des données. Plusieurs standards de facto, nationaux ou internationaux gravitent aujourd'hui autour de ce domaine: ISF/SoGP, OIT/ISG, BS 15000 (ITIL), BS 7799, ISO 17799, ISO 13335, etc. Nous nous sommes penchés sur le standard international ISO 17799:2000 (Code of Practice for Information Security Management), ainsi que sur son pendant britannique BS 7799-2:2002 (Information Security Management Systems). Le premier constitue un référentiel très complet (CoP: Code of Practice) permettant de définir les mesures techniques et organisationnelles de sécurisation de l'information, en fonction du risque que le maître de fichier (l'en-

treprise) estime supportable. ISO 17799 comporte dix objectifs de sécurité, formellement numérotés de trois à douze et dont le premier constitue le fondement absolu de la norme:

- *la politique de sécurité de l'information*
- la sécurité organisationnelle (infrastructure, accès par des tiers, externalisation…)
- la classification et la maîtrise des actifs (étiquetage, manipulation…)
- la sécurité du personnel (responsabilités, formation, sanctions lors d'abus…)
- la sécurité physique et environnementale (locaux, équipements, généralités)
- la gestion des communications et opérations (procédures, capacité, maliciels, travaux de routine, réseau, manutention des supports-mémoire, échanges d'information)
- le contrôle d'accès (besoins, utilisateurs, mots de passe, services réseau, systèmes d'exploitation, applications, supervision, appareils portables et télétravail)
- le développement et la maintenance des systèmes (applications, cryptographie, mises à jour et correctifs, données de test…)
- la gestion de la continuité des affaires (plan, test, maintenance)
- la conformité (exigences légales, techniques, issues de la politique; journalisation)

Le premier objectif, soit la politique de sécurité de l'information, est le document central qui contient un ensemble de buts stratégiques et conceptuels portant sur la sécurité globale de l'information d'une organisation. Parmi les objectifs intermédiaires, il est réjouissant de constater que la majorité des problèmes soulevés par les nouvelles technologies de l'information et de la communication sont pris en compte.

Le dernier objectif revêt pour nous un intérêt prépondérant, car il inclut les aspects de conformité avec les exigences légales, en particulier celles de la protection des données. Un accent spécifique peut ainsi être mis sur les principes essentiels que sont le respect de la licéité, de la transparence, de la proportionnalité et de la finalité des traitements, l'exactitude des données, le droit d'accès ou encore le devoir de déclaration des fichiers. Les fichiers de journalisation, qui contiennent des données relatives à des personnes identifiées ou identifiables, devraient donc impérativement être traitées conformément à ces principes.

Ce standard international permet ainsi de pondérer les mesures de protection et sécurité des données en fonction du contexte d'application. Sur cette base, il est ensuite naturel de recourir au standard britannique BS 7799-2 pour mettre sur pied un

système de gestion de la sécurité de l'information. Un tel système peut alors faire l'objet d'un audit, afin de déterminer si le traitement de l'information répond bien aux exigences attendues. C'est dans cet esprit que s'inscrit le nouvel article 11 proposé dans le cadre de la révision actuelle de la LPD et portant sur une procédure de certification (organisations ou produits) en matière de protection des données.

2.1.3 Traces électroniques sur la place de travail

Les activités effectuées sur ordinateur laissent des traces électroniques, dont une partie contient des données personnelles. La collecte et le traitement de celles-ci sont soumis à la LPD.

Aujourd'hui la plupart des tâches professionnelles et privées sont effectuées à l'aide d'un ordinateur. Toutes ces activités laissent des traces électroniques, à partir desquelles il est théoriquement possible de reconstruire les actions de l'utilisateur (qui, quoi et quand). Le potentiel d'intrusion dans la sphère privée est important.

La LPD s'applique aux données personnelles contenues dans les catégories de traces électroniques suivantes:

- Les fichiers journaux (logfiles);
- Les fichiers temporaires: *.TMP, Index.dat et témoins de connexion (cookies);
- La base de registres et les fichiers de configuration (*.INI);
- Les historiques: système d'exploitation, navigateur, applications, etc.;
- Les presse-papiers (clipboards);
- Les corbeilles;
- Les archives personnelles (*.PST);
- Les copies de sauvegarde (backups).

La question de l'effacement logique ou physique des données se pose également. Les données effacées logiquement d'un support informatique pouvant être aisément récupérées, il est recommandé d'utiliser des effaceurs physiques écrasant les données personnelles par réécriture multiple.

Une entreprise peut traiter des traces électroniques afin de vérifier le respect des directives relatives à l'utilisation des ressources informatiques et l'efficacité des mesures de sécurité. Les logiciels produisant en règle générale des traces électroniques, il est impératif de déterminer les normes de protection des données applicables dans ce cas. La LPD exige le respect des règles suivantes:

- But du traitement clairement défini par le maître de fichier;
- Absence d'autres solutions moins intrusives mais tout aussi efficaces;
- Transparence par rapport aux personnes concernées;
- Collecte des seuls éléments nécessaires au but fixé;
- Respect de la période de conservation prévue;
- Analyses selon des procédures prédéfinies et vérifiables;
- Sécurisation de toutes les données traitées;
- Mécanisme préétabli pour l'exercice du droit d'accès.

Les analyses des fichiers journaux doivent être clairement réglées. Il s'agit de la partie la plus délicate en raison du risque élevé d'accès non autorisés aux données personnelles. Pour éviter des abus, les analyses doivent être effectuées par un groupe restreint de personnes (en principe les administrateurs). Les administrateurs chargés de cette tâche seront contrôlés par une personne indépendante et de confiance (par exemple le conseiller à la protection des données).

Dans le cas des logiciels produisant des fichiers journaux, le principe de transparence voudrait que leur existence soit clairement indiquée aux personnes concernées. Afin de contribuer au respect de la proportionnalité, la production de ces fichiers journaux devrait être une option du logiciel, désactivée par défaut. Dans tous les cas, les logiciels devraient offrir la possibilité d'effacer les données journalisées.

Pour plus de détails, voir le document «Traces électroniques et protection des données» publié par le PFPD (http://www.edsb.ch/f/themen/sicherheit/technik/elektronische_spuren_f.pdf).

2.1.4 Protection de son propre ordinateur

L'utilisation de l'ordinateur pour le courrier, le commerce et la banque électronique ou tout simplement pour la recherche d'informations représente une activité quotidienne. La plupart des personnes se connectant à Internet ne réalisent pas que cette opération peut mettre en péril la sécurité de leur installation et de leurs données. La prise de conscience des risques possibles est le premier pas vers une autoprotection, réalisable en recourant à des logiciels le plus souvent gratuits.

Une première catégorie de risques est constituée par les *traces électroniques*. Les activités exécutées sur l'ordinateur laissent des traces qui, si elles sont analysées

correctement, permettent de reconstruire les actions de l'utilisateur. Il sera ainsi possible de dévoiler les adresses des pages Internet visitées, les courriels envoyés et reçus, ainsi que toute une série d'autres données personnelles pouvant même conduire à l'établissement d'un profil de personnalité. L'attaque de ces données ne passe pas nécessairement par un accès physique à l'ordinateur, étant donné que ces traces peuvent être aussi collectées via Internet.

La deuxième catégorie de risques est constituée par les *atteintes à la sécurité*. Le but de ce genre d'attaque est le vol, l'insertion, la mutation ou la destruction de données ou encore la paralysie de l'ordinateur. Le cas typique est un virus ou une page Internet ouvrant en cascade des dizaines de fenêtres publicitaires. Dans cette catégorie il y a aussi le polluriel (spam), qui surcharge un compte de courrier électronique parfois jusqu'à le rendre inutilisable.

Enfin il y a encore la catégorie des *risques économiques*. Par exemple un maliciel (hijacker) qui remplace le numéro habituel du fournisseur d'accès à Internet par un numéro de service à valeur ajoutée (090x) plus cher et cela à l'insu de la personne concernée.

Pour minimiser les risques, il est possible de se doter de logiciels de protection le plus souvent gratuits:

- *Antivirus*: la possibilité d'être infecté par des virus est haute, notamment en cas de téléchargement des logiciels. Un bon antivirus, mis à jour régulièrement, constitue une protection indispensable.
- *Trace eraser*: certaines traces électroniques persistent après l'utilisation d'un ordinateur. L'effacement de ces traces est parfois très compliqué et l'utilisation de logiciels ad hoc est conseillée.
- *Cookie manager*: les témoins de connexion sont des traces qui peuvent être utiles, mais aussi servir de clé pour voler des données. Un bon gestionnaire de témoins (cookie manager) permet une gestion effective par l'utilisateur.
- *Antispyware*: un spyware est un logiciel qui peut collecter à l'insu de la personne concernée des données personnelles pour un tiers. Un antispyware mis à jour régulièrement prévient ce genre d'attaque.
- *File wiper*: en lieu et place de l'effacement par défaut logique, les données personnelles peuvent être détruites au moyen d'un effaceur physique (file wiper).
- *Personal firewall*: lors d'une connexion à Internet, un attaquant peut chercher à s'introduire dans votre ordinateur. Des éléments actifs incontrôlables d'une page Internet (java, javascript, ActiveX, etc.) peuvent en outre être exécutés à votre insu. Un pare-feu personnel (personal firewall) limite ce genre d'attaque.

- *Antispam*: les polluriels (spam) engorgent les comptes de courrier électronique avec de la publicité. Les logiciels antispam évitent par filtrage «intelligent» des courriels entrant une bonne partie de ces nuisances.
- *Antidialer*: un tel logiciel prévient le remplacement intempestif du numéro du fournisseur habituel par un numéro de service à valeur ajoutée plus onéreux. La décision de l'Office fédéral de la communication d'interdire l'utilisation de PC-Dialers en liaison avec les numéros 090x constitue une bonne parade à ce genre de problème. Des PC-Dialers, par exemple en liaison avec des numéros satellitaires, peuvent cependant subsister, c'est pourquoi un antidialer est toujours recommandé.
- *Antibanner*: certaines pages Internet ouvrent en cascade des dizaines de fenêtres truffées de publicité qui dérangent considérablement l'utilisateur. Un antibanner limite ce genre de désagrément.

2.1.5 Nécessité de crypter les données enregistrées sur un disque dur (ou autre support de données), en particulier dans les environnements sensibles

Lorsqu'un médecin ou autre professionnel qui traite des données personnelles sensibles doit par exemple faire réparer son ordinateur, le technicien qui effectue la réparation est en mesure de consulter, voire de traiter les données stockées sur cet ordinateur. Si les données sont chiffrées, il est pratiquement impossible pour le technicien d'accéder à ces données.

Nous recevons régulièrement des demandes pour savoir comment se comporter lorsqu'un ordinateur personnel ou un disque dur doit être réparé pour éviter que les données stockées ne puissent être consultées par des tiers, tels que des techniciens informatiques. En particulier les médecins, notaires et avocats traitent des données personnelles très sensibles. Mais aussi les utilisateurs privés d'ordinateurs personnels conservent sur leurs propres systèmes des informations qui ne regardent personne d'autre, surtout pas le technicien chargé de la réparation. Pensons par exemple aux données de la déclaration d'impôts ou à d'autres notices personnelles. Les dispositions légales prévoient que les données personnelles sensibles et les profils de la personnalité ne peuvent être traitées que si les mesures de sécurité prises sont à la pointe de la technique. Cela signifie entre autres que de telles données ne peuvent être enregistrées sur disque dur que sous forme cryptée. L'utilisation de procédés de cryptage est particulièrement simple dans des environnements informatiques de taille réduite. Dans les cas où un disque dur doit être réparé ou si l'ordinateur personnel est volé, tout tiers non autorisé qui ne connaît pas le mot (ou l'expression) de passe ou ne possède pas la carte à puces permettant de décrypter les données enregistrées, ne sera pas en mesure d'accéder à ces données.

Souvent, des systèmes informatiques ou des parties de tels systèmes sont revendus après une certaine période d'utilisation. Dans un tel cas, les données enregistrées doivent être supprimées de manière à ce qu'elles ne puissent pas être reconstruites. Souvent, les programmes standard de suppression des données n'effectuent qu'une suppression logique des données, ce qui signifie que ces dernières peuvent relativement aisément être reconstruites si elles n'ont pas été écrasées. Si les données sensibles ont été enregistrées sous forme cryptée, puis supprimées physiquement, il n'est pas nécessaire d'écraser les données par inscription répétitive de configurations binaires puisque le cryptage originel des données effacées rend une reconstruction des données d'autant plus difficile. Une sécurité absolue ne peut cependant être atteinte que si l'on détruit physiquement le disque dur ou support de données de telle manière à ce qu'il ne soit plus possible de reconstruire les données.

2.1.6 Journalisation des activités de systèmes en production

Une journalisation doit être effectuée dans les domaines où la protection ou la sécurité des données ne peut pas être assurée par des mesures préventives. Un tel domaine est par exemple l'accès à un système informatique par des collaborateurs internes ou externes qui possèdent des droits d'accès élevés, tels que les responsables systèmes, les administrateurs de banque de données, etc.

Une journalisation doit être effectuée notamment dans les domaines dans lesquels des mesures préventives (telles que le cryptage des données) ne suffisent pas pour assurer la sécurité nécessaire des données. Une journalisation ne permet cependant d'enregistrer que ce qui s'est déjà passé. Cela signifie qu'au moment où l'on découvre une violation de la protection des données dans le journal, celle-ci a déjà eu lieu. Ces journalisations ont néanmoins un effet préventif, puisque les utilisateurs ou exploitants du système savent que certaines activités sont journalisées. Il y a lieu donc de communiquer aussi clairement que possible à toutes les personnes concernées quelles activités sont journalisées et pourquoi. En fonction du système, il peut être nécessaire de procéder à plusieurs journalisations. Un principe important est de n'enregistrer que le strict nécessaire, pour éviter d'accumuler d'énormes volumes de données que plus personne n'est en mesure de dépouiller. Il est en outre judicieux de concevoir les journaux de manière à ce que les données soient enregistrées de manière uniquement anonymisée ou au moins pseudonymisée. Il n'est normalement pas nécessaire lors du dépouillement d'un journal de pouvoir identifier un utilisateur individuel. Le dépouillement devrait se faire de manière aussi anonyme que possible, permettant uniquement d'identifier une unité administrative telle qu'un office, une

division ou une section. Il est important de chercher à concevoir le système de manière à ce que des mesures préventives ne permettent qu'un travail conforme à la protection des données, ne laissant ainsi que quelques rares domaines «ouverts» aux mesures de journalisation. Un tel domaine «ouvert» est par exemple l'accès à un système informatique par des collaborateurs internes ou externes qui possèdent des droits d'accès élevés, tels que les responsables systèmes, les administrateurs de banque de données, etc. pour autant que ceux-ci aient un accès libre aux données, c.-à-d. que celles-ci ne soient pas physiquement ou logiquement isolées. Un tel environnement présente un risque accru, étant donné que toutes les données enregistrées sont accessibles. Les données enregistrées dans les journaux doivent satisfaire aux exigences de la révision. Cela signifie notamment que ces fichiers doivent être conçus de manière à ce qu'ils ne puissent pas, après coup, être manipulés ou supprimés de manière incontrôlée. Il faut en outre tenir compte de l'exigence que les données ainsi enregistrées ne peuvent être conservées que pour une durée limitée.

2.2 Autres thèmes

2.2.1 Questionnaire médico-psychologique accompagnant le recrutement

A l'occasion de leur recrutement, les conscrits doivent remplir un questionnaire médico-psychologique dont le but est d'évaluer leur aptitude au service militaire. Les questions portant sur la sexualité surtout ont donné lieu à maints commentaires. Néanmoins, la plupart des autres questions interviennent aussi dans la sphère privée et intime des conscrits. Les réponses à ces questions constituent de ce fait des données sensibles ou des profils de la personnalité. Un traitement de données aussi sensibles par une autorité n'est licite que si certaines conditions sont respectées. Il incombe fondamentalement au Parlement de décider si ce genre de test d'aptitude peut être utilisé.

Depuis peu, les conscrits doivent remplir un long questionnaire à l'occasion des journées de recrutement. Selon les commentaires du DDPS figurant sur Internet, ce questionnaire a pour but d'évaluer aussi l'aptitude psychique des conscrits au service militaire, outre leur aptitude médicale. Le questionnaire comporte d'après le DDPS environ 400 questions dont six questions sur la sexualité. Selon le DDPS, la sexualité constitue un comportement fondamental de l'être humain et la manière dont elle est vécue peut avoir une influence sur la santé psychique de la personne. Les conscrits doivent répondre à toutes les questions.

Les questions concernant la sexualité surtout ont fait l'objet de maints commentaires dans les médias. Nous avons été contactés par de très nombreuses recrues inquiètes et préoccupées ainsi que par leurs familles. Nous avons immédiatement pris contact avec les services responsables du DDPS et requis de plus amples informations à ce sujet.

Sur la base des comptes-rendus dans les médias et des dires des conscrits qui se sont adressés directement à nous, nous avons constaté les points suivants:

Les réponses aux questions sur la sexualité constituent des données personnelles sensibles. De nombreuses autres questions parmi les 394 autres constituent aussi des données sensibles (par ex. questions sur la santé, sur des mesures d'aide sociale, sur d'éventuelles poursuites et sanctions administratives ou pénales). Etonnamment, ce fait n'a d'ailleurs rencontré que peu d'écho dans les médias.

Les réponses permettent d'évaluer des aspects essentiels de la personnalité des conscrits. Nous sommes donc en présence d'un profil de la personnalité au sens de la LPD.

Du fait de leur contenu sensible, seules quelques réponses à peine suffisent à établir un profil de la personnalité. Ce qui est douteux, c'est que le conscrit doit répondre à des questions concernant des tierces personnes comme les parents, les grands-parents ou les frères et sœurs. Ces questions ne sont licites qu'en présence du consentement des personnes concernées.

Nous avons profité d'une séance avec les services compétents du DDPS pour exposer en détail et clairement la position du PFPD:

Un test d'aptitude médico-psychologique, ordonné par une autorité étatique, empiète sur la sphère privée et intime du citoyen.

La décision de savoir si une autorité est habilitée à utiliser ce genre de tests d'aptitude doit toujours être précédée d'un débat au niveau social et politique. Seul le Parlement est légitimé à décider en procédure législative ordinaire de la nécessité et de l'opportunité de ces tests.

Le traitement de données sensibles et de profils de la personnalité doit être prévu expressément dans une loi fédérale.

Les principes du traitement des données doivent être mentionnés dans la loi fédérale. Ce sont les suivants:

- la définition du but du traitement;
- la description non détaillée de l'ampleur que prendra le traitement des données (point qui doit être clair pour la personne concernée);

- la détermination des personnes participant au traitement des données (personnes traitant les données, destinataires des données);
- la mention des catégories des données traitées (dans la mesure où des données sensibles ou des profils de la personnalités sont concernés).

Ce n'est qu'à partir du moment où les bases légales suffisantes sont données qu'une autorité administrative peut élaborer ce genre de tests d'aptitude et les mettre en œuvre.

Dans le cas présent, comme dans tout traitement de données, les principes généraux de la protection des données doivent être strictement respectés au cours de chaque phase (proportionnalité des questions, transparence lors du traitement des données, finalité, etc.).

Etant donné le caractère sensible des données, il convient d'accorder une attention particulière au principe de la transparence. Les conscrits doivent être informés exactement des buts du questionnaire, des personnes qui ont accès aux réponses, de la durée de conservation des données, de l'éventualité de la transmission des réponses à des tiers, etc.

2.2.2 Publication de photos et de noms dans les systèmes électroniques d'accès

Les systèmes électroniques d'accès et de contrôle tels que ceux qui sont utilisés dans les domaines skiables ou autres installations sportives ne doivent pas afficher des données telles que le nom ou la date de naissance sur un écran qui est visible du public. Pour autant qu'il n'existe pas d'autre possibilité de contrôle, il est permis exceptionnellement d'afficher la photo du détenteur légitime à des fins de contrôle, mais seulement à proximité immédiate du point de contrôle.

Les skieurs se voient confrontés de plus en plus à des systèmes modernes d'émissions de billets et de contrôle d'accès qui traitent également des données personnelles. A l'achat de billets, surtout de cartes d'abonnement qui ont une longue durée de validité, on enregistre de manière numérique non seulement les données personnelles du client, mais aussi sa photo. Cette démarche a pour but de contrôler que les billets personnels sont vraiment utilisés uniquement par leur détenteur et non pas par une tierce personne.

Dans certains domaines skiables, les données personnelles sont également visibles pour le public qui se trouve dans l'enceinte du système de contrôle d'accès. Au moment où le client traverse le tourniquet, sa photo ou plus précisément celle du déten-

teur légitime s'affiche sur un grand écran. Parfois, d'autres données telles que le nom, le prénom ou la date de naissance s'affichent également. Le but de cette mesure est d'enrayer les utilisations abusives, notamment l'utilisation de cartes personnelles par d'autres personnes que le détenteur légitime. Le système permet ainsi un contrôle par les autres skieurs. Des cas où l'affichage a duré plusieurs minutes nous ont été rapportés.

La mise en œuvre de tels systèmes doit toujours tenir compte du principe de la proportionnalité. L'atteinte à la personnalité des personnes concernées doit se limiter à ce qui est absolument nécessaire pour endiguer les abus. On donnera la préférence à d'autres systèmes de contrôle qui sont plus réservés en ce qui concerne le traitement de données, notamment à ceux qui rendent moins de données accessibles à des tiers. Un exemple pourrait être les contrôles ponctuels des billets par le personnel. Si l'on opte pour un système qui enregistre les photos des clients, on cherchera une solution dans laquelle le contrôle visuel est effectué par le personnel sur un écran de contrôle situé dans un local séparé et non visible du public.

Si les conditions locales ne permettent pas d'autre possibilité de contrôle, un affichage de courte durée (quelques secondes) de la photo et si nécessaire du numéro de billet du détenteur légitime dans la zone d'accès public peut être accepté. L'écran doit toutefois se trouver à proximité immédiate du point de contrôle et ne doit pas être visible par l'ensemble de la file d'attente. L'affichage visible par le public de données supplémentaires telles que nom, prénom et date de naissance ou autres informations est par contre disproportionné.

Dans tous les cas, les clients doivent être informés clairement au moment de l'enregistrement de leurs données sur le traitement prévu ainsi que sur sa finalité.

3. Justice/ Police/ Sécurité

3.1 Affaires de police

3.1.1 Reconnaissance faciale dans les stades

Le recours à un système de reconnaissance faciale constitue un traitement de données personnelles. Si les données sont traitées par des personnes privées, celles-ci doivent disposer d'un motif justificatif et respecter les principes fondamentaux de la protection des données. Il est impératif dans tous les cas d'informer clairement les personnes concernées afin de les rendre attentives au système de reconnaissance faciale, ainsi qu'à la possibilité d'exercer leur droit d'accès. Il se pose en outre le problème de la coordination, ainsi que celui de la répartition des compétences et des tâches entre les organes privés d'une part, auxquels incombent certaines mesures de sécurité, et les organes de police d'autre part, auxquels incombe le maintien de la sécurité publique. Tous les autres détails doivent être clairement réglés avant la mise en œuvre d'un système de reconnaissance faciale.

Nous avons été consultés sur l'opportunité d'installer un système de reconnaissance faciale dans les stades. Toutefois, en l'absence d'indications concrètes, nous n'avons pu nous exprimer que de manière très générale sur cette question du point de vue de la LPD.

En premier lieu, il faut se référer à l'aide-mémoire du PFPD sur la vidéosurveillance effectuée par des personnes privées (cf. notre 8ème Rapport d'activités 2000/2001, paragraphe 3.1 et annexe 3). Toutefois, la mise en œuvre d'un système de reconnaissance faciale soulève également d'autres questions. De plus, il ne faut pas oublier qu'actuellement les systèmes de reconnaissance faciale sont encore entachés d'un taux d'erreur élevé. Ceci provoquerait parfois des situations où des spectateurs aucunement impliqués (c'est-à-dire non présents dans la base de données) seraient incorrectement identifiés comme personnes enregistrées pour comportement violent. Pour les personnes concernées, cela signifierait une atteinte inadmissible à leur personnalité et constituerait en outre une violation du principe de l'exactitude des données. Ces aspects ne doivent certainement pas être négligés avant l'introduction d'un système de reconnaissance faciale.

Le système de reconnaissance faciale, tout comme la surveillance vidéo des spectateurs, constitue un traitement de données personnelles. Il faut donc tenir compte de la législation sur la protection des données. Au niveau fédéral, c'est la LPD qui est

applicable lorsque des organes fédéraux ou des personnes privées traitent des données. Si des organes fédéraux traitent des données personnelles, ceci requiert en outre une base légale. De même, selon les lois cantonales sur la protection des données, une base légale est requise pour le traitement de données par les organes cantonaux.

Dans le cas de la présente demande, on pouvait admettre que les données seraient traitées par des associations (personnes privées). Des personnes privées ne sont en droit de traiter des données personnelles que si elles disposent d'un motif justificatif, à savoir le consentement de la personne concernée, un intérêt public ou privé prépondérant ou une loi. De plus, les principes fondamentaux de la protection des données doivent être respectés (notamment les principes de licéité, de bonne foi, de proportionnalité, de finalité, l'exactitude et la sécurité des données ainsi que le droit d'accès). Ainsi, les données ne peuvent être collectées que de manière licite et, selon le principe de la proportionnalité, seules pourront être traitées les données qui sont nécessaires et appropriées au but poursuivi. Il faut vérifier dans chaque cas particulier si ces conditions sont satisfaites.

En ce qui concerne les motifs justificatifs, ce sont surtout l'intérêt public prépondérant dans le cadre de mesures de sécurité ainsi que le consentement des personnes concernées qui entreront en ligne de compte. Dans tous les cas, une information claire des personnes concernées s'impose – que ce soit sur les billets d'entrée ou ailleurs – afin de les rendre attentives à la présence d'un système de reconnaissance faciale, ainsi qu'à la possibilité d'exercer leur droit d'accès.

Un autre problème qui se pose est celui de la coordination ainsi que de la répartition des compétences et des tâches entre les organes privés d'une part (équipes locales ou à la rigueur la FIFA), auxquels incombent certaines mesures de sécurité, et les organes de police d'autre part, qui sont responsables de maintenir la sécurité publique. Selon la formule retenue, il faudrait éventuellement créer encore des bases légales. Il existe actuellement au niveau fédéral un projet de loi sur les mesures contre le racisme et l'hooliganisme (cette loi sera intégrée à la loi existante sur les mesures visant au maintien de la sûreté intérieure). Ce projet de loi ne prévoit en fait pas le recours à un système de reconnaissance faciale, mais par contre l'introduction d'un «fichier des hooligans».

Finalement, tous les autres détails devraient être clairement réglés avant la mise en œuvre d'un système de reconnaissance faciale. Il s'agirait en particulier de régler les conditions sous lesquelles une personne est enregistrée dans la base de données, quelles données sont communiquées, à quelles conditions et à qui (police, autres clubs de football etc.), où et combien de temps les données sont conservées et à quel

moment elles sont supprimées, qui a accès à ces données, qui est chargé du traitement des demandes d'accès, comment les personnes concernées (particulièrement les spectateurs) sont informées sur l'utilisation d'un tel système etc. Lors de la détermination de ces conditions, on observera les principes fondamentaux de la loi sur la protection des données mentionnés plus haut, dont le principe de proportionnalité. Le plus judicieux serait de fixer ces détails dans un règlement de traitement (ou dans une loi si les données sont traitées par une organe fédéral ou cantonal).

3.2 Autres thèmes

3.2.1 Ordonnance sur la vidéosurveillance CFF

L'ordonnance du 5 décembre 2003 sur la vidéosurveillance des Chemins de fer fédéraux (CFF) est entrée en vigueur le 1er janvier 2004. Cette ordonnance constitue la base légale exigée par la LPD pour les traitements de données personnelles effectués dans le cadre des activités de surveillance au moyen de caméra vidéo des installations ferroviaires des CFF et des trains exploités par ces derniers. Nos remarques concernant la protection de la sphère privée ont été prises en compte lors de l'élaboration de cette ordonnance, notamment celles relatives à l'information des personnes concernées, à l'accès aux données et à leur durée de conservation. Nous avions déjà demandé l'élaboration d'une telle norme lors de l'introduction, à titre d'essai, de caméras de surveillance dans une rame du trafic régional (voir notre 8ème Rapport d'activités 2000/2001, paragraphe II.3.2) et à la suite de notre contrôle relatif à la vidéosurveillance effectuée par les CFF dans la gare principale de Zurich (voir notre 9ème Rapport d'activités 2001/2002, paragraphe 3.2.2 et notre 10ème Rapport d'activités 2002/2003, paragraphe 3.2.3).

3.2.2 Code de procédure civile et loi sur la protection des données

Dans le cadre de la consultation des offices relative au projet d'experts pour un code de procédure civile unifié sur le plan suisse, nous avons pris position en particulier sur les modifications prévues de l'art. 15 LPD en ce qui concerne les droits des personnes concernées. Il s'agit pour nous notamment d'assurer que la référence à certains droits continue de figurer dans la LPD même.

Dans le cadre de la consultation des offices, nous avons pu prendre position sur le projet d'experts pour un code de procédure civile unifié pour l'ensemble de la Suisse (CH-CPC). Le projet d'experts CH-CPC prévoit notamment une modification de l'art. 15 de la LPD, qui règle les droits des personnes concernées (prétentions et procédure). Dans notre prise de position, nous faisions remarquer que la LPD se trouve actuellement en révision et que celle-ci touche aussi l'art. 15 LPD qui subit une légère modification. Il s'agissait donc d'assurer que le projet d'experts CH-CPC se base sur le projet de révision de la LPD.

Nous suggérions de renoncer aux modifications de l'art. 15, al. 1 LPD prévues dans le rapport d'experts CH-CPC et de maintenir la référence aux articles 28 à 28l du code civil qui constitue un instrument important du droit de la personnalité. Il est en outre important, comme jusqu'alors, de faire expressément référence dans la LPD même au droit d'exiger le blocage, la rectification ou la destruction des données. Il faut aussi maintenir explicitement dans la LPD (art. 15, al. 4 LPD) l'application d'une procédure simple et rapide aux actions relatives au droit d'accès. La LPD resterait ainsi lisible et compréhensible pour le profane.

Par ailleurs, nous demandions de faire expressément référence dans l'art. 15, al. 3 LPD à la possibilité d'exiger le blocage de toute communication de données à des tiers, comme le prévoit le projet de révision de la LPD.

4. Informatique et télécommunication

4.1 Exploitation de caméras web conforme aux exigences de la protection des données

Internet connaît les caméras web depuis plusieurs années déjà et la question de savoir si leur exploitation est conforme à la protection des données resurgit régulièrement. En résumé, il existe deux possibilités d'utiliser ces caméras de manière légale: soit les caméras sont installées et configurées de manière à ce qu'aucune personne ne soit identifiée ou identifiable, soit les personnes concernées donnent leur consentement à être filmées.

Les images de ces caméras web sont accessibles sur Internet dans le monde entier, elles peuvent être traitées (enregistrées, imprimées, transmises etc.) sans aucun contrôle. Leur qualité varie en fonction du système utilisé: certaines caméras sont installées de manière fixe et ne permettent pas à l'usager de choisir un angle de prise de vue. D'autres caméras par contre sont dirigeables par l'utilisateur ou lui permettent de faire un zoom sur un plan. Selon la technique utilisée et la position de la caméra, il est possible de reconnaître des personnes sur ces prises de vue. Souvent, les caméras installées ne sont pas perçues par les personnes filmées. Ces dernières n'ont donc pas connaissance du fait qu'elles sont prises en image, ni à quelle fin et surtout elles ignorent complètement que leur image peut être captée dans le monde entier par le biais d'Internet. Pour autant que les images accessibles ne fournissent aucune information permettant d'identifier une personne, aucune objection ne peut être faite du point de vue de la protection des données. S'il est possible par contre d'identifier une personne, nous nous trouvons en présence d'un traitement de données personnelles au sens de la LPD. Une personne est aussi identifiable dans les cas où les données fournies ne l'identifient pas directement, mais que les circonstances, c'est-à-dire le contexte de l'information (tel que certains objets, l'habillement, un véhicule etc.) permettent de conclure à l'identité de la personne.

Quiconque traite des données personnelles est tenu de respecter notamment les principes suivants de la LPD: les données personnelles doivent être collectées de manière licite; leur traitement doit respecter les règles de la bonne foi et être proportionnel; les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. Il n'est cependant pas autorisé de communiquer des données personnelles à l'étranger si ceci peut constituer une atteinte grave à la personnalité des personnes concernées, notamment parce qu'une protection des données équivalente à celle qui est garantie en Suisse fait défaut dans les pays en question.

Toute personne privée qui traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Une atteinte à la personnalité lors d'un traitement de données personnelles par une personne privée est contraire à la loi si elle n'est pas justifiée par le consentement de la personne concernée, par un intérêt privé ou public prépondérant ou par la loi. Les exploitants de caméras web ne peuvent pas faire valoir un tel intérêt. D'autre part, aucune disposition légale pour l'exploitation de caméras web n'est donnée. Cela signifie que des données personnelles récoltées par une caméra web ne peuvent être traitées qu'avec le consentement des personnes concernées. Celui-ci doit être donné librement et en connaissance de toutes les circonstances. Si la personne concernée doit craindre certains préjudices au cas où elle refuserait de se laisser filmer, le consentement est considéré comme nul. Souvent, l'obtention d'un tel consentement est impraticable (par ex. pour des caméras web installées sur la voie publique). Dans ce cas, il y a lieu de garantir par des mesures techniques et organisationnelles que les personnes prises en image ne puissent pas être identifiées ou identifiables.

En résumé, les utilisations suivantes de caméras web sont conformes aux exigences de la protection des données:

- La caméra web est installée de manière à ce qu'aucune personne (ni objet qui permettrait d'identifier une personne) ne puisse être reconnue.
- Au cas où une identification serait possible, la personne qui se trouve dans l'angle de prise de vue de la caméra doit donner son consentement. La volonté de ne pas être filmé doit être respectée en tout temps. De plus, une information claire, qui n'est soumise à aucune condition doit avoir lieu avant que la personne n'entre dans l'angle de prise de vue de la caméra.

Nous avons demandé à plusieurs exploitants de systèmes de caméras web en Suisse de vérifier la conformité de leurs installations avec la législation en matière de protection des données et de l'adapter si nécessaire. Pour des raisons de capacité, nous ne sommes pas en mesure de procéder à des contrôles systématiques des caméras web. En cas d'atteinte à leur personnalité, les personnes concernées sont libres d'introduire une action civile.

5. Santé

5.1 Enregistrements vidéo de patientes et patients à des fins de supervision et de formation

Le traitement de données personnelles par des cliniques privées est soumis à la LPD. Des enregistrements vidéo de patients contiennent des données personnelles particulièrement sensibles et sont à considérer comme des profils de la personnalité. Le traitement de telles données à des fins de supervision et de formation ne se justifie que difficilement. S'il est autorisé, la procédure doit être réglée avec un caractère obligatoire. Le patient doit donner son consentement écrit pour l'enregistrement et l'utilisation des bandes vidéo. La responsabilité de la protection des données incombe à la clinique qui produit et utilise les bandes vidéo.

Une clinique psychiatrique privée souhaite utiliser des enregistrements vidéo de patients à des fins de supervision et de formation. L'enregistrement, l'utilisation, la conservation et la transmission de tels enregistre-ments font l'objet d'un règlement. Pour l'élaboration de ce règlement, nous avons fait parvenir à la clinique les considérations sui-vantes.

Le traitement de données personnelles par des cliniques privées est soumis à la LPD. Les enregistrements vidéo constituent un traitement de données au sens de la LPD. Ils contiennent d'une part des données personnelles sensibles (données médicales) et constituent d'autre part des profils de la personnalité, c'est-à-dire qu'ils permettent d'apprécier des aspects essentiels de la personnalité. La clinique doit, comme pour tout traitement de données, respecter les principes fondamentaux de la LPD et faire valoir un motif justificatif (consentement, intérêt prépondérant ou loi).

La responsabilité pour la mise en œuvre des principes de traitement des données de la LPD incombe toujours à celui qui traite les données, dans le cas présent à la clinique. Elle doit évaluer tous les risques du traitement de données prévu et procéder à la nécessaire pesée des intérêts.

Deux principes fondamentaux de la LPD sont le principe de proportionnalité et celui de la finalité. Ils doivent être respectés lors de tout traitement de données. La proportionnalité existe si le traitement est approprié et nécessaire à but prévu, et si celui-ci ne peut pas être obtenu par un autre traitement de données touchant moins au droit de la personnalité de la personne concernée. Le traitement de données personnelles sensibles et de profils de la personnalité constitue une atteinte grave au droit de la personnalité. Une telle atteinte à des fins de supervision et de formation peut à peine se justifier. Si même il peut avoir lieu, un tel traitement ne sera donc autorisé que dans

un cadre limité et à des conditions clairement définies. Il y a lieu de considérer que les patients séjournent dans la clinique dans un tout autre but, soit pour recouvrer leur santé. La supervision et la formation poursuivent par contre d'autres buts, à savoir le conseil individuel dans le contexte du travail concret d'un professionnel (p.ex. un thérapeute) ou la formation et le perfectionnement professionnel.

Il est du devoir de la clinique d'apprécier la proportionnalité lors de l'utilisation d'enregistrements vidéo, une appréciation séparée étant requise pour chaque usage prévu.

Le principe de proportionnalité exige que dans tous les cas où un rapport avec la personne ne doit pas absolument être établi, on procède systématiquement à une anonymisation ou tout au moins à une pseudonymisation des données personnelles. Les données anonymes perdent le caractère de données personnelles et leur traitement n'est plus soumis à la LPD. Une anonymisation complète n'existe cependant que lorsque tout rapprochement avec la personne concernée est exclu, donc lorsque celle-ci n'est absolument plus identifiable. En pratique, on recourt souvent à une «barre sur les yeux» pour rendre une personne méconnaissable, ce qui ne permet toutefois d'obtenir une anonymisation suffisante que dans une minorité des cas. Dans les enregistrements vidéo, il faut p.ex. s'assurer que l'environnement est neutre, que les voix sont déformées et que ni des visages, ni d'autres caractéristiques identifiantes ne sont visibles. Là aussi, l'appréciation peut se présenter différemment en fonction du but. Alors que pour la supervision une faible, voire même aucune dissimulation de l'identité de la personne concernée peut à la rigueur encore être proportionnelle, un degré d'anonymisation bien plus grand est nécessaire dans le cas d'enregistrements utilisés à des fins de formation. On peut toutefois douter qu'il soit même possible d'atteindre une anonymisation complète des enregistrements vidéo dans le domaine de la psychiatrie. Il est probable que les entretiens enregistrés évoquent souvent des circonstances et événements si spécifiques et importants pour le cas en question que ceux-ci ne pourront pas simplement être filtrés sans trop vider le contenu de son sens ou le déformer.

Un autre aspect de la proportionnalité est le délai d'utilisation des enregistrements vidéo. Une utilisation pour une durée indéterminée n'est pas conciliable avec le principe de proportionnalité, quand bien même le patient y consentirait. Le consentement pour un traitement de données disproportionné n'est pas possible et n'est pas non plus légalement valable. Lorsque le but est atteint (p.ex. au terme de la supervision), un autre usage ou la conservation des bandes n'est plus justifié. L'emploi à des fins de formation doit lui aussi être limité dans le temps. Comme il s'agit de données personnelles sensibles et de profils de la personnalité, il ne peut s'agir que d'une période de quelques mois.

Le principe de proportionnalité exige en outre que le cercle des personnes qui ont connaissance de données personnelles sensibles ou de profils de la personnalité soit restreint autant que possible. Pour les enregistrements vidéo destinés à la formation, cette condition ne peut forcément pas être respectée.

Après avoir pesé les intérêts en jeu, la clinique doit décider dans quel cadre et avec quelles restrictions elle entend autoriser les enregistrements vidéo. Eu égard à la sensibilité de tels enregistrements, un règlement détaillé s'avère indispensable. Il incombe à la clinique, en tant qu'instance procédant au traitement des données, la responsabilité de la protection des données et il lui revient de s'assurer que les enregistrements sont utilisés de manière proportionnelle et appropriée (p.ex. uniquement pour des formations professionnelles spécialisées et seulement si les enregistrements pour la formation présentent réellement une utilité supplémentaire).

Comme motif justificatif pour des enregistrements vidéo à des fins de supervision et de formation, seul le consentement du patient concerné entre en ligne de compte. S'il s'agit du traitement de données personnelles sensibles ou de profils de la personnalité, le consentement est soumis à des exigences particulièrement élevées. Plus les données à traiter sont délicates, plus l'information à la personne concernée doit être détaillée et plus le consentement doit s'effectuer clairement (cf. notre 7ème Rapport d'activités 1999/2000, paragraphe 3.1).

La personne consentante doit être en mesure d'estimer l'étendue et la portée de son consentement. Elle doit être capable de discernement quant à l'enregistrement et l'utilisation de telles bandes vidéo. Le consentement d'une personne non capable de discernement n'est pas légalement valable. Le représentant légal peut cependant consentir à sa place.

A des fins de preuve et du fait de la sensibilité des données traitées, le consentement doit être donné par écrit. Pour la validité juridique du consentement, il est déterminant que la personne concernée ait été informée sur ses droits et sur les traitements de données prévus. Il est donc indispensable de remettre au patient une notice d'information circonstanciée qui décrit l'utilisation prévue de manière détaillée et compréhensible, depuis le moment de l'enregistrement jusqu'à l'effacement des bandes.

L'information au patient doit contenir une description précise du but de l'enregistrement vidéo. Si plusieurs buts sont poursuivis, ceux-ci seront énumérés séparément. Le patient doit aussi savoir si et comment les enregistrements seront anonymisés pour les différents buts. Cette information est importante pour la décision du patient de donner son consentement pour tous les buts prévus ou seulement certains d'entre eux. Si plusieurs buts sont prévus, le patient doit avoir la possibilité de choisir. On peut imaginer que quelqu'un est d'accord de faire des enregistrements pour la super-

vision, mais ne souhaite pas que ces enregistrements soient également utilisés à des fins de formation.

Tant que les enregistrements restent en possession du personnel médical, ils sont protégés dans une très large mesure par le secret professionnel. Toutefois, si les enregistrements entrent en possession d'autres personnes, ce qui en soi serait admissible sur la base d'un consentement approprié du patient, ils ne se trouvent plus sous la protection du secret professionnel. La notice d'information doit clairement mentionner cela. De même, elle mentionnera aussi les dispositions que prend la clinique pour maintenir les bandes vidéo et leur contenu sous la protection du secret professionnel.

Selon la LPD, le patient peut en tout temps demander quelles sont les données traitées à son sujet. Par le droit d'accès, l'ayant droit est en mesure de faire valoir d'autres droits relatifs à la protection des données (rectification, anonymisation ou destruction de données plus utilisées, dans le cas présent surtout l'effacement de la bande vidéo). Une référence à ces droits figurera également dans la notice d'information. De plus, le patient devra aussi savoir à qui adresser la demande d'accès.

Il est également important de mentionner expressément le caractère volontaire des enregistrements vidéo et le fait qu'un refus du consentement n'a pas de conséquences préjudiciables pour le patient. Un consentement donné peut être révoqué en tout temps sans indication du motif. Si un patient vient à révoquer son consentement, les enregistrements ne peuvent plus être utilisés dès ce moment. La clinique doit garder le contrôle sur l'utilisation des bandes (où et quand) afin qu'elle puisse le cas échéant les récupérer et en ordonner l'effacement. Le patient peut demander une confirmation de l'effacement. Une remise des bandes vidéo au patient plutôt qu'un effacement est envisageable pour des enregistrements individuels.

Pour les enregistrements de groupes, le consentement de chacune des personnes impliquées est requis. Dans de tels cas aussi, le consentement doit être de plein gré, c'est-à-dire qu'il ne doit pas en résulter de contrainte de fait (pression du groupe). Même si une seule des personnes impliquées révoque son consentement, la bande vidéo doit être effacée. La remise à un ou plusieurs patients (copies vidéo) est soumise à l'accord de toutes les personnes impliquées.

La pratique soulève également souvent des questions sur les rapports de propriété. Cette question devrait donc être traitée dans le règlement. Elle concerne la propriété de la cassette. Les données personnelles qui y sont enregistrées «appartiennent» cependant dans tous les cas aux personnes concernées. Celles-ci peuvent faire valoir leurs droits à ce sujet indépendamment des rapports de propriété sur la cassette. Il s'agit également de régler ce qu'il advient des cassettes lorsque le patient ou le

méde-cin traitant quitte la clinique. Ainsi, on peut inclure dans le règlement un principe (p.ex. effacement de l'enregistrement), auquel il serait également possible de déroger avec un accord écrit à ce sujet de toutes les personnes impliquées. La réglementation peut différer pour les enregistrements à des fins de supervision et les enregistrements à des fins de formation.

Les explications données s'appliquent par analogie à toutes les personnes concernées outre le patient (thérapeutes). Les enregistrements vidéo à des fins de surveillance sont régis par l'aide-mémoire correspondant du PFPD.

5.2 Secret professionnel et encaissement par un tiers des factures d'honoraires avec poursuite éventuelle du patient

Le secret professionnel interdit aux médecins de communiquer des données de patients à des tiers. Si un médecin désire charger une caisse de médecins de l'encaissement de ses factures d'honoraires ou s'il se voit contraint d'engager une poursuite contre un patient mauvais payeur, il a besoin du consentement de ce patient. Dans le cas de la poursuite, on peut aisément imaginer que le patient donnera que rarement son accord. Pour les cas où la personne concernée ne donne pas son consentement, mais que le médecin nécessite dans son intérêt personnel que son obligation de maintenir le secret soit levée, la loi prévoit la possibilité d'une libération du secret professionnel par l'autorité dont il relève ou par l'autorité de surveillance. Le médecin ne peut pas invoquer le consentement implicite du patient.

Il est aujourd'hui courant de faire appel à des institutions professionnelles pour des travaux administratifs. La LPD permet un traitement de données par des tiers, pour autant que le mandant veille à ce que ne soient pas effectués de traitements autres que ceux qu'il est lui-même en droit d'effectuer et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

L'attribution par des médecins de mandats à des tiers, p.ex. à des caisses de médecins ou bureaux d'encaissement, se heurte à l'obligation légale de garder le secret, à savoir le secret professionnel réglementé par le code pénal (secret médical). La divulgation à des tiers de données concernant un patient n'est donc autorisée que si le consentement du patient existe, une loi le prévoit ou l'autorité de surveillance en a donné l'autorisation au médecin. La formulation dans le code pénal est claire et précise à ce sujet. Il est incontesté aujourd'hui que le seul fait d'une visite chez le médecin en soi tombe déjà sous le secret médical. Dans le cas des données nécessaires à l'encaissement ou à la poursuite, il s'agit donc toujours de données sensibles.

Un médecin qui veut charger une caisse de médecins de l'encaissement de ses honoraires a donc besoin du consentement de son patient. En pratique, le consentement du patient s'obtient normalement avant le début du traitement au moyen d'un formulaire, sur lequel le patient signe une déclaration de consentement préformulée. Nous avons toutefois constaté que les déclarations de consentement utilisées sont souvent rédigées de manière insuffisamment précises.

Qu'en est-il alors du cas où un patient mauvais payeur doit être poursuivi ? Du fait que là aussi des données sensibles doivent être transmises au bureau d'encaissement mandaté ou à l'office des poursuites, il est nécessaire que le médecin soit libéré du secret professionnel. Aux termes de la loi, ne sont envisageables que le consentement du patient ou la libération par l'autorité dont relève le médecin, ou par l'autorité de surveillance. Le consentement pourrait bien être obtenu préventivement au début du traitement au moyen du formulaire déjà mentionné. Une telle démarche n'est toutefois pas très habile psychologiquement – le patient se sentirait étiqueté dès le début comme non-payeur potentiel – et c'est pourquoi en pratique ce consentement n'est soit même pas demandé, soit pas fourni par le patient. Il est peu probable que le patient donne son consentement plus tard, lorsque la poursuite s'avère nécessaire.

On nous pose par conséquent souvent la question si, dans le cas où une poursuite devient nécessaire, plutôt que de faire libérer le médecin du secret médical par l'autorité dont il relève, il ne serait pas permis pour des raisons de praticabilité de conclure à un consentement implicite, dans la mesure où le patient ne réagit pas à la menace écrite expresse d'engager une poursuite.

Comme le consentement n'est pas lié à une forme prescrite, il peut également être donné implicitement. Le consentement implicite se distingue du consentement explicite en ceci qu'il résulte de l'ensemble des circonstances de manière reconnaissable et patente. Le comportement du patient doit donc être absolument concluant. Les circonstances, en l'occurrence le silence du patient, ne permettent toutefois pas de conclure sans autre à un consentement implicite. Premièrement, il résulte déjà du principe de proportionnalité que le consentement doit être d'autant plus clair que les données sont sensibles (cf. notre 7ème Rapport d'activités 1999/2000, paragraphe 3.1). Deuxièmement, il faut considérer que, lors du recouvrement de ses honoraires, le médecin agit non pas dans l'intérêt du patient, mais dans son propre intérêt. Précisément dans les cas où la personne concernée ne donne pas son consentement, mais où le médecin dépend – pour son intérêt personnel – de la levée de l'obligation au secret, le législateur a expressément prescrit la voie passant par l'autorité dont dépend le médecin. Troisièmement, selon la jurisprudence du Tribunal fédéral, une simple dette d'argent ne peut pas justifier une violation des droits fondamentaux, ici sous forme d'une atteinte à la personnalité par la communication de données.

Pour toutes ces raisons, un consentement implicite ne suffit pas, tant pour l'externalisation administrative de la facturation, que pour la poursuite du patient qui serait un mauvais payeur. Il est en outre dans l'intérêt du médecin de disposer d'un consentement écrit explicite du patient ou d'une autorisation écrite de l'autorité dont il dépend, car il s'expose à une plainte pénale s'il devait s'appuyer lors de la communication de données à des tiers sur un consentement insuffisant ou non valable légalement.

Les deux cas sont comparables en ce qui concerne la nécessité et la clarté du consentement du patient. En pratique, il est important que les déclarations de consentement appropriées soient formulées séparément et sans équivoque, de sorte que le patient puisse donner librement un ou les deux consentements. Ci-dessous, une formulation possible:

Je donne au Dr XY mon accord pour transmettre à l'office d'encaissement (nom/adresse) les données requises pour l'établissement et l'encaissement des factures.

Lieu, date: ..... Signature: .....

Je suis d'accord/pas d'accord (biffer ce qui ne convient pas) qu'en cas de retard de paiement de ma part, le Dr XY ou l'office d'encaissement (nom/adresse) mandaté par ses soins puisse engager et exécuter le recouvrement de la dette auprès de l'office des poursuites compétent.

Je prends connaissance du fait qu'en l'absence de ce consentement, le médecin a la possibilité de demander à l'autorité dont il relève ou à l'autorité de surveillance la levée du secret professionnel afin d'engager le recouvrement de la dette.

Lieu, date: ..... Signature: .....

6. Assurances

6.1 Assurances sociales

6.1.1 Réglementations lacunaires dans le domaine de la protection des données médicales

Le rapport sur la protection des données médicales dans le domaine des assurances sociales a été soumis à l'Office fédéral des assurances sociales (OFAS) et au PFPD (voir le postulat 00.3178 de la Commission des affaires juridiques du Conseil national). Il est important que notre avis soit pris en considération dans la procédure de consultation qui va suivre.

L'OFAS a été invité, dans un postulat, à élaborer un rapport complet sur la protection des données médicales dans l'ensemble du secteur des assurances sociales. Nous avons été invités à collaborer à ces travaux (pour plus de détails, se reporter à notre 10ème Rapport d'activités 2002/2003, paragraphe 6.1.2). Ce rapport doit en particulier souligner et analyser les possibilités et les risques de l'évolution technologique du traitement électronique des données. Le secret médical tel qu'il figure dans le code pénal a constitué le point de départ des travaux. La rédaction finale du rapport a été effectuée par l'Institut du droit de la santé de l'Université de Neuchâtel.

L'OFAS nous a soumis le rapport (non encore publié) pour une première appréciation. L'OFAS et nous-mêmes défendons des opinions différentes sur le contenu du rapport. Les divergences portent sur la manière de remédier aux lacunes touchant l'exécution des dispositions de protection des données dans le secteur des assurances sociales.

L'OFAS mènera prochainement une procédure de consultation auprès des milieux concernés (assureurs, organisations de patients, etc.). Nous présumons que nous aurons également la possibilité de nous prononcer. Il est important pour nous que notre appréciation soit directement intégrée dans le rapport ou soit soumise séparément au Parlement.

6.1.2 La SUVA et le recours à des détectives privés

La filature et la surveillance vidéo d'assurés par la SUVA ne sont possibles qu'à certaines conditions. Ces mesures nécessitent notamment une base légale réglementant clairement le but et la portée de ce genre de surveillance.

La filature et la surveillance vidéo des assurés est un thème de plus en plus présent dans les activités quotidiennes du PFPD. La question du recours à des détectives

privés s'est posée au cours de l'année écoulée surtout avec la SUVA (cf. ATF 5C 187/1997 et question ordinaire Leutenegger Oberholzer 03.1077: contrôle et surveillance vidéo d'assurés). La SUVA agit en tant qu'assureur accidents obligatoire.

Nous n'ignorons pas qu'en matière d'assurance-accidents obligatoire, les services des détectives privés sont de plus en plus utilisés. Le but de leurs investigations est d'éviter ou de découvrir les éventuelles demandes de prestations injustifiées des assurés. Ces recherches soulèvent certaines questions du point de vue de la protection des données (nous n'entrerons pas en matière sur leur aspect pénal).

Les photos et les enregistrements vidéo d'assurés (y compris l'élaboration de rapports) constituent des traitements de données au sens de la LPD. Ils impliquent une atteinte grave aux droits de la personnalité des assurés. Cela d'autant plus lorsque des données médicales sont traitées sans que les personnes concernées en soient informées au préalable.

Les organes de la Confédération - comme dans le cas présent de l'assurance-accidents obligatoire - ne sont généralement en droit de traiter des données personnelles comme les filatures et les surveillances vidéo que s'il existe une base légale ad hoc. Par ailleurs, les principes de la protection des données comme la transparence et la proportionnalité doivent être respectés dans toute la mesure du possible. Nous sommes d'avis que dans toute la législation sur les assurances sociales, il n'y a aucune norme légale qui permettrait de justifier le recours à des détectives privés.

En outre, les filatures et les surveillances vidéo effectuées par les assurances-accidents obligatoires doivent être dans l'intérêt public et surtout répondre au principe de la proportionnalité. Ainsi, il serait difficile de placer systématiquement plus haut par exemple les intérêts financiers de l'assurance-accidents que les droits de la personnalité des assurés. Il est néanmoins très important de veiller à ce que les assurances-accidents prennent tout d'abord, dans le cadre de leur devoir d'investigation, d'autres mesures portant moins atteinte à la sphère privée. Les filatures ou les surveillances vidéo des assurés doivent être nécessaires et, de ce fait, constituer le seul moyen de pouvoir découvrir un abus en matière d'assurance. En outre, les surveillances secrètes d'assurés ne doivent pas être effectuées à titre préventif, mais doivent reposer sur un motif concret de soupçon quant à un abus éventuel de prestations non justifiées.

Il est fondamentalement permis de douter que les filatures et les surveillances vidéo soient le moyen permettant le mieux de détecter un éventuel abus en matière d'assurance. En particulier la valeur probatoire de ce genre d'enquêtes, qui ne constituent que des relevés momentanés, est probablement limitée.

Nous estimons que la question des filatures et des surveillances vidéo par les assurances-accidents n'est pas encore résolue de manière satisfaisante du point de vue de la protection des données et nécessite une analyse plus approfondie. Il convient surtout de vérifier si les filatures et les surveillances vidéo dans le domaine des assurances-accidents permettent de faire véritablement le point sur les demandes de prestation des assurés. Si tel était effectivement le cas, il conviendrait de créer une base légale qui règle de manière claire le but, la portée et les conditions de ces méthodes de surveillance. Dans tous les cas, il convient d'éviter que de nouveaux moyens de preuve ou de nouvelles méthodes soient admises purement et simplement dans le domaine de l'assurance-accidents. Il pourrait en ressortir la tendance selon laquelle la fin justifie les moyens.

6.2 Assurances privées

6.2.1 La collecte de données personnelles par les assurances-responsabilité civile

Nous avons mis au point des normes minimales à propos des conditions dans lesquelles une assurance-responsabilité civile est en droit de requérir une expertise sur une personne lésée. La mesure doit être justifiée et la personne doit en avoir été informée au préalable de manière complète. Nous avons rassemblé ces principes dans un aide-mémoire également consultable sur Internet (voir à l'adresse http://www.edsb.ch/f/doku/merkblaetter/haftpflicht.htm ainsi qu'à l'annexe 13.4 du présent rapport).

6.2.2 Lutte contre l'abus en matière d'assurance et protection des données

Les assureurs privés renforcent leurs moyens de lutte contre l'abus en matière d'assurance. Or, souvent, ils entrent en conflit avec la législation sur la protection des données.

Les assureurs privés mettent actuellement en place des structures dont le but est de détecter les pratiques frauduleuses. Il existe depuis des années déjà un système central d'information (le ZIS) mis au point par l'Association suisse d'assurances (ASA) et accessible à toutes les compagnies d'assurance. Le ZIS est un fichier, enregistré auprès du PFPD, sur les procédures pénales et civiles pendantes et closes (pour plus de détails à ce sujet, cf. notre 7ème Rapport d'activités 1999/2000, paragraphe 7.9). Les assureurs pour leur part ont pris des mesures permettant de lutter contre l'abus en

matière d'assurance. Ils ont par exemple recours à des détectives privés pour contrecarrer les éventuelles demandes de prestations injustifiées des assurés. Nous avons été confrontés à ce genre de cas à plusieurs reprises au cours de l'année écoulée.

Les assurances privées sont soumises à la législation sur la protection des données et doivent donc en respecter les prescriptions lorsqu'elles procèdent à des investigations. Elles doivent en particulier respecter les principes de la protection des données tels que la sécurité des données, le principe de la proportionnalité et le principe de la transparence.

Dans un cas, il a été découvert par hasard qu'un assureur privé gérait depuis quelques années des fichiers internes. Les personnes fichées n'étaient pas au courant de l'existence de ces fichiers, lesquels n'étaient du reste pas annoncés auprès du PFPD. Ces «listes noires» concernent d'une part le domaine des assurances privées et d'autre part le domaine de l'assurance-maladie et de l'assurance-accidents. Ces banques de données ont pour objectifs, entre autres, de permettre une vue d'ensemble sur les mesures de lutte contre l'abus en matière d'assurance. Elles contiennent des données personnelles sensibles comme les poursuites pénales. L'assurance en question a annoncé ses deux fichiers auprès du PFPD.

Nous procédons aussi actuellement à d'autres éclaircissements. Nous avons entre autres prié l'assureur de prendre les mesures qui s'imposent du point de vue technique et organisationnel. Il faut par exemple que les personnes non autorisées ne puissent pas accéder aux fichiers. Un autre problème se pose, celui de la catégorie de données «Remarques générales», qui peuvent être utilisées de manière abusive pour y insérer des écrits susceptibles de léser la personnalité des personnes concernées.

Le problème majeur aujourd'hui est néanmoins le manque de transparence des fichiers mentionnés. Un fichier comparable au casier judiciaire de l'Etat doit être connu de la personne concernée. Les fichiers contenant des données personnelles sensibles doivent donc être annoncés auprès du PFPD. Les «listes noires» dans ce domaine sensible ne sont donc pas prévues par le législateur et sont même punissables dans certaines circonstances. L'actuelle révision de la LPD prévoit même de donner plus de poids au principe de la transparence. Ainsi, un devoir d'information direct à l'égard des personnes concernées doit donc être introduit lorsque des données personnelles sensibles sont traitées.

6.2.3 Le projet de révision de la LSA et de la LCA

Le Conseil fédéral a adopté le message concernant la révision de la loi sur la surveillance des assurances (LSA) et de la loi sur le contrat d'assurance (LCA). Ces modifications prévoient également une amélioration de la protection des données dans le domaine des assurances privées.

Après plusieurs consultations des offices, le Conseil fédéral a publié un projet de révision de la loi sur la surveillance des assurances et de la loi sur le contrat d'assurance. L'objectif premier de ces travaux législatifs est la sécurité des entreprises d'assurance et une meilleure protection des consommateurs. Les principales remarques du PFPD à cet égard ont été prises en considération.

L'un des objectifs de la protection des consommateurs est le renforcement du devoir d'information des assureurs. Le projet de LCA prévoit donc que les assureurs sont tenus d'informer les preneurs d'assurance du contenu essentiel du contrat d'assurance. Cette obligation recouvre également l'information sur le traitement des données personnelles, y compris le but et le genre de fichier ainsi que les destinataires et la conservation des données. De même, selon la version révisée de la LSA, les intermédiaires d'assurances doivent aussi informer les assurés du traitement des données. Nous approuvons entièrement le fait que le traitement des données deviennent plus transparent pour les preneurs d'assurance et assurés. En effet, le manque de transparence du traitement des données est effectivement l'un des problèmes majeurs dans le domaine des assurances privées.

Par ailleurs, le projet de LSA oblige les entreprises d'assurance à mettre sur pied des organes externes de révision. Cet organe externe doit immédiatement informer l'autorité de surveillance lorsqu'une entreprise d'assurance lèse entre autres les intérêts des assurés. Selon le texte du message, les intérêts des assurés sont également lésés lorsqu'il y a violation de prescriptions en matière de protection des données. Ce qui signifie que l'Office fédéral des assurances privées doit intervenir d'office en qualité d'autorité de surveillance également en cas d'atteintes à la protection des données.

Nous apprécions les efforts visant à améliorer la protection des données dans le domaine des assurances privées. Il reste à espérer que dans le cadre de l'actuelle révision totale de la LCA, un poids encore plus grand sera accordé aux intérêts de la protection des données. Nous avons attiré l'attention de la commission d'experts chargée de la révision totale de la LCA sur les différents problèmes et possibilités de solution. Nous considérons comme une excellente base à cet égard la Recommandation du Conseil de l'Europe sur la protection des données à caractère personnel col-

lectées et traitées à des fins d'assurance. Cette recommandation prévoit par exemple que le traitement de données médicales ne doit être effectué que par des professionnels de la santé. Nous continuerons à suivre les travaux concernant la révision totale de la LCA.

7. Secteur du travail

7.1 Les aspects juridiques d'une permanence téléphonique de collecte des plaintes

Une entreprise désire mettre en place, à l'intérieur de ses propres structures, une permanence téléphonique de collecte des plaintes chargée de la constatation et de la poursuite des comportements illicites ou contraires à l'éthique dans l'entreprise. Celle-ci est tenue d'en informer les employés. Cette permanence doit être fiable, neutre et impartiale. Elle doit traiter tous les participants sur un pied d'égalité et les protéger dans leur personnalité.

Une société internationale nous a fait part de son projet de créer une permanence interne chargée de collecter les plaintes. Elle permettrait aux employés comme aux tiers extérieurs de s'adresser anonymement à elle pour signaler un comportement problématique du point de vue éthique ou juridique de la part de l'entreprise ou de l'un de ses collaborateurs. Sans dévoiler son identité, un employé pourrait donc se plaindre d'une personne précise. Il serait préservé d'une confrontation directe tant avec le collaborateur en question qu'avec l'entreprise. Le but serait de lui permettre de s'exprimer librement et ouvertement de faits posant problème, comme le harcèlement sexuel sur le lieu de travail. Par ailleurs, l'anonymat le préserverait de tout mobbing ou de toute menace.

Nous avons informé l'entreprise que l'anonymat permet aussi au dénonciateur de dénigrer de manière injustifiée un collaborateur, tout en étant lui-même totalement protégé. Ainsi, une telle permanence téléphonique peut involontairement favoriser la dénonciation abusive. La personne accusée se trouve dans une position vulnérable et totalement exposée vis-à-vis du dénonciateur anonyme. Elle peut éventuellement certes faire valoir un droit de réponse à l'égard de l'entreprise, mais une confrontation équitable et transparente avec le dénonciateur anonyme n'est pas possible.

Par exemple, il ne serait pas possible d'entamer une poursuite contre le dénonciateur pour calomnie ou délit contre l'honneur. L'égalité de traitement du dénonciateur et du collaborateur dénoncé n'est pas garantie en raison du déséquilibre des forces. Pour combattre cela, le dénonciateur doit indiquer des coordonnées, au moins sous forme d'adresse électronique non nominative. En cas de besoins, l'identité complète doit aussi être communiquée à la permanence. Cette mesure devrait au minimum permettre une prise de contact et, le cas échéant, une confrontation avec la réponse de l'employé accusé. Si la possibilité de contact manque, il ne devrait en principe pas être entré en matière sur la plainte.

L'impartialité et la neutralité de la permanence ainsi que le caractère confidentiel de son action ont pour but de protéger les personnes concernées de préjudices tels que les préjugés ou le mobbing au sein de l'entreprise. Dans l'idéal, la permanence devrait être indépendante. Cela pourrait néanmoins avoir des répercussions négatives en ce sens que des faits sensibles devraient être communiqués à une entreprise tierce moyennant rétribution. Une solution de compromis pourrait être la suivante: chaque filiale de ce groupe international met à disposition un représentant au sein d'une permanence téléphonique commune. Les appels concernant une filiale ne devraient être pris et traités que par le représentant d'une autre filiale. Une certaine impartialité et neutralité pourraient ainsi être garanties.

Au préalable, il convient d'informer expressément les employés de l'existence et du but d'une permanence indépendante chargée de recevoir les plaintes. En effet, ce genre de structure génère des traitements de données et les personnes concernées ont un droit d'accès, qui peut être invoqué en tout temps, également sans indice concret de plainte. Outre le droit d'accès, le droit de rectification et le droit de destruction des données doivent être garantis aux personnes concernées. Si l'employeur devait recevoir, par l'intermédiaire de la permanence, des informations personnelles pour des motifs relevant du droit du travail, il serait tenu de les traiter confidentiellement, à l'instar de la permanence. La communication de données à des tiers (par ex. aux collègues de travail de la personne concernée) par l'employeur n'est pas admise ou uniquement en présence d'un intérêt prépondérant. Dès que le but du traitement des données est rempli, les données doivent être détruites. L'enregistrement d'appels téléphoniques sur supports de son est régi par les dispositions du code pénal. En vertu de celles-ci, la personne qui, sans le consentement des autres participants, aura écouté à l'aide d'un appareil d'écoute ou enregistré sur un porteur de son une conversation non publique entre d'autres personnes, ou enregistré sur un porteur de son une conversation non publique à laquelle il prenait part sera puni de l'emprisonnement ou de l'amende.

7.2 Décision de la Commission fédérale de la protection des données en matière de dépistage de la consommation de drogues auprès des apprentis

Après transmission de notre recommandation à la CFPD (cf. notre 9ème Rapport d'activités 2001/2002, paragraphes 7.8 et 13.6.3), la décision attendue a été rendue fin août 2003. Elle confirme dans une large mesure la position défendue dans notre recommandation. Selon cette décision donc, la société Roche doit adapter son concept de dépistage de la consommation de drogue auprès des apprentis en ce sens que ces dépistages ne doivent désormais plus avoir lieu que dans des cas isolés et uniquement si le consentement de la personne en question a été donné. Selon la CFPD, toutes les données relevées jusqu'ici dans le cadre du concept susmentionné doivent être détruites dans la mesure où il n'y a pas de soupçon fondé d'abus. La décision de la CFPD figure dans le présent rapport (annexe 13.9).

7.3 Recommandation du PFPD au sujet de la liste de licenciements d'Orange

L'entreprise Orange SA a établi une liste de ses employés devant servir de base à un licenciement collectif. Cette liste contenait des appréciations, pour certaines subjectives, portant sur le comportement des employés ainsi que des données inadéquates et disproportionnées relevant de la sphère privée. Les employés concernés n'ont pas été informés de l'existence de cette liste. Nous avons recommandé à Orange SA d'en informer les personnes concernées et de garantir le droit d'accès. Par ailleurs, nous avons recommandé de ne conserver cette liste que jusqu'à l'entrée en force d'éventuelles décisions judiciaires. Par ailleurs, nous avons invité Orange SA, si d'autres licenciements collectifs devaient être décidés à l'avenir, de garantir la protection contre la résiliation du contrat de travail, l'égalité des droits, la liberté syndicale et l'égalité entre femmes et hommes, et de se limiter aux catégories de données qui sont nécessaires et appropriées au déroulement correct d'un licenciement collectif. La recommandation figure dans le présent rapport (annexe 13.10.1).

7.4 Explications sur la vidéosurveillance sur le lieu de travail

L'expérience a montré que les installations de vidéosurveillance suscitent des sentiments négatifs chez les employés ainsi contrôlés et compromettent l'ambiance générale de travail. Elles peuvent porter atteinte au bien-être, à la santé psychique et ainsi qu'au rendement du personnel. Nos explications sur la vidéosurveillance sur le lieu de travail viennent compléter l'aide-mémoire sur la vidéosurveillance effectuée par

des personnes privées (cf. http://www.edsb.ch/f/doku/merkblaetter/video.htm). Elles figurent dans le présent rapport (annexe 13.1).

7.5 Explications sur la surveillance des communications téléphoniques sur le lieu de travail

Depuis l'apparition des téléphones mobiles dans le monde du travail, il est apparu nécessaire de remplacer l'aide-mémoire publié en 1999 par le groupe de travail des préposés cantonaux et du préposé fédéral à la protection des données sur l'utilisation du téléphone sur le lieu de travail. Les explications du PFPD figurent dans le présent rapport (annexe 13.2).

7.6 Explications sur les prises de références lors d'une candidature

La doctrine et la pratique divergent quant à la délivrance de références. La controverse porte essentiellement sur le fait de savoir si les références ne doivent être données qu'avec le consentement du candidat. On avait espéré une solution avec l'entrée en vigueur de la LPD. La situation juridique et la pratique sont néanmoins demeurées incertaines. Nos explications ont pour objectif de clarifier cette question. Les explications sur les prises de références lors d'une candidature peuvent être consultées sur Internet à l'adresse http://www.edsb.ch/f/themen/weitere/referenzauskuenfte_f.pdf et figurent également dans le présent rapport (annexe 13.3).

8. Economie et commerce

8.1 Modification de l'art. 179quinquies du code pénal: pas de punissabilité pour l'enregistrement de certaines conversations téléphoniques

Le 1er mars 2004, la nouvelle version de l'art. 179quinquies du code pénal (CP) est entrée en vigueur. Cette modification permet désormais d'enregistrer certaines conversations téléphoniques dans le cadre des relations d'affaires sans l'accord des participants. Cette disposition d'exception est néanmoins rédigée dans un sens très restrictif et les enregistrements ne doivent être utilisés qu'à des fins de preuve.

Avec l'entrée en vigueur de la nouvelle version de l'art. 179quinquies CP, l'enregistrement de conversations téléphoniques n'est plus punissable dans deux cas:

- lorsque la conversations implique des services d'assistance, de secours ou de sécurité (art. 179quinquies, al. 1, let. a); et
- lorsque la conversation enregistrée porte sur des commandes, des mandats, des réservations ou d'autres transactions commerciales de même nature, dans le cadre de relations d'affaires (art. 179quinquies, al. 1, let. b).

Selon la disposition en vigueur jusqu'ici, seul l'enregistrement d'appel d'urgence n'était pas punissable. Dans le cadre de la présente modification, une question surtout s'est posée: l'impunité désormais prévue délie-t-elle également de l'obligation de transparence imposée par le droit de la protection des données et de ce fait de l'obligation d'informer les interlocuteurs concernés ?

L'analyse de l'objectif poursuivi par cette modification tel qu'il ressort des débats parlementaires montre que le législateur entendait clairement permettre les enregistrements dans des situations de conversations particulières, supprimant l'obligation de requérir le consentement des personnes concernées et donc de les informer au préalable. Du point de vue de la LPD, la présente modification du code pénal signifie que celui qui traite des données dans les cas prévus par la nouvelle disposition peut se prévaloir d'un motif justificatif (la loi) au sens de l'art. 13, al. 1 LPD.

Selon la nouvelle disposition, les conversations téléphoniques impliquant des services d'assistance, de secours ou de sécurité peuvent être enregistrées même s'il ne s'agit pas d'appels d'urgence. La non-punissabilité de l'enregistrement n'est pas limitée aux appels portant sur un numéro spécial (numéro d'urgence). Il n'est pas nécessaire d'informer au préalable la personne qui appelle. Les conversations peuvent être enregistrées par tous les participants.

Au cours des délibérations aux Chambres fédérales, la formulation de l'exception pour les relations d'affaires a été fortement restreinte par rapport à la proposition d'origine. La genèse de cette nouvelle disposition montre clairement que celle-ci se rapporte à des situations de conversation très précises.

Selon l'al. 1, let. b, il n'est possible d'enregistrer une conversation sans information préalable que dans le cadre de *commandes, de mandats, de réservations ou d'autres transactions commerciales de même nature.* Le Conseil national a précisé qu'il s'agit de relations en masse. L'abandon de l'obligation d'informer dans ces cas a été motivé par le fait que dans certaines situations, il serait trop long et laborieux de signaler l'enregistrement aux interlocuteurs, notamment dans le domaine du tourisme. La dépénalisation visée par le législateur avec cette modification se limite donc à des situations dans lesquelles une affaire particulière s'effectue en masse et où une certaine rapidité est nécessaire à son bon fonctionnement. Ainsi, l'enregistrement de conversations par le biais d'un numéro de téléphone de commande ou de réservation bénéficie clairement de la nouvelle disposition.

Par contre, dans le cas d'un contrat négocié au téléphone par exemple, il est tout à fait possible, raisonnablement exigible et proportionné que celui qui veut enregistrer la conversation en informe son interlocuteur. Même lorsqu'un rapport contractuel existe déjà entre les deux interlocuteurs, une information préalable doit avoir lieu. Effectivement, l'expérience a déjà montré qu'une mention de l'enregistrement dans les conditions générales ou dans le cadre d'un contrat ne pose aucun problème.

La portée de la clause d'exception a été également explicitée par les chambres à l'aide d'exemples: ainsi, il est possible d'enregistrer une conversation sans information préalable lorsqu'il s'agit de réservations de billets d'avion ou de chambres d'hôtel. En revanche, il sera nécessaire d'informer l'interlocuteur de l'enregistrement d'une conversation relative à une réclamation concernant un vol ou une chambre d'hôtel.

En ce qui concerne tous ces enregistrements désormais possibles sans information préalable, il convient néanmoins de respecter une *stricte finalité* dans leur utilisation. Ils ne peuvent être utilisés que pour leur valeur de preuve. La communication de tels enregistrements à des tiers reste notamment punissable et il convient en particulier de souligner que l'*exploitation* de tels enregistrements n'est pas permise. Ainsi, il est exclu que des enregistrements effectués en vertu de la nouvelle disposition d'exception soient analysés à des fins de marketing. Dans les cas où une telle exploitation doit avoir lieu ou que les enregistrements doivent être utilisés à des fins de formation ou pour le contrôle du comportement de vente des employés, une information préalable demeure nécessaire.

8.2 Publicité non désirée: droit de suppression de ses données personnelles

Il ne doit pas y avoir de traitement de données personnelles contre la volonté expresse de la personne concernée. Celle-ci peut exiger que le responsable du traitement des données lui confirme que les informations la concernant ont été effacées. En cas de récidive, il faut également communiquer à la personne concernée qui a transmis ses données pour qu'elle puisse aussi requérir la suppression de ses données en amont.

Un particulier nous a contactés et informés qu'il était régulièrement sollicité par une communauté religieuse, bien qu'il lui ait déjà signifié à plusieurs reprises par écrit qu'il ne voulait plus recevoir de courrier de sa part. Il a également exigé que cette communauté le raye de ses listes d'adresses. Etant donné que plusieurs personnes se sont déjà plaintes auprès de nous de cette institution, nous sommes intervenus et lui avons signalé clairement les dispositions légales précises existant à ce propos.

Conformément à la LPD, une personne peut exiger expressément que ses données personnelles ne soient pas traitées contre sa volonté et que toutes les données la concernant dans le fichier de la personne qui procède au traitement soient effacées. Elle peut en outre demander que le responsable du traitement lui confirme que les données ont bien été effacées. Le responsable du traitement est tenu de prendre les mesures qui s'imposent du point de vue technique et organisationnel pour que la volonté de cette personne soit respectée. A titre de conséquence logique, le responsable du traitement est donc habilité dans ce but (mais uniquement dans ce but) à établir une liste des données personnelles (nom et adresse) des particuliers ne désirant à l'avenir plus être contactés.

Nous avons mis cette communauté religieuse en demeure de confirmer au particulier concerné et à nous-même l'effacement des données. Nous lui avons prescrit en outre de prendre les mesures nécessaires pour que la volonté expresse de tous ceux qui ne souhaitent plus être contactés, par écrit également, soit respectée et que les principes de la LPD soient observés.

Par ailleurs, nous avons attiré son attention sur le fait que le responsable du traitement doit en cas de récidive informer la personne concernée de la raison pour laquelle il n'a pas été tenu compte de sa demande ou auprès de qui son adresse a été obtenue. Pour la personne concernée, c'est la seule manière d'imposer l'effacement de son adresse également auprès du fournisseur d'adresses.

Si le responsable du traitement ne respecte pas la volonté expresse de la personne contactée et continue de la relancer, cette personne peut déposer une plainte pour violation de la protection de la personnalité. En outre, au cas où le responsable d'un traitement de données ne se conformerait pas à l'injonction qui lui a été faite de ne plus contacter une personne déterminée, nous nous réservons expressément le droit de procéder à un contrôle.

8.3 Transmission de données clients émanant d'un rapport de confiance

Le principe de la transparence revêt une importance particulière lors de la transmission, au sein d'une entreprise, de données clients émanant d'un rapport de confiance. Seul le client qui a connaissance du fait que le cercle des responsables du traitement des données et les modalités de traitement convenues à l'origine vont être modifiés est en mesure d'autoriser la transmission. Son consentement doit être donné expressément et devrait même avoir lieu par écrit s'il s'agit de données sensibles ou de profils de la personnalité.

Dans le cadre d'un projet de réorganisation, un établissement financier avait l'intention de fermer un centre de consultation dans la ville A et de l'intégrer à celui de la ville B, au sein d'une nouvelle unité d'organisation. Il nous a priés d'examiner si la transmission des données clients était autorisée. Ces données étaient, aux dires de l'entreprise, d'une part des données sensibles (entre autres des données médicales) et d'autre part des profils de la personnalité (liste exhaustive de la situation patrimoniale des clients).

Le principe fondamental à respecter dans le cas présent est le principe de la bonne foi (principe de transparence). Selon ce principe, la collecte des données et tout autre traitement de données doivent être transparents pour la personne concernée, c'est-à-dire être reconnaissables en tant que tels. En d'autres termes, les données ne doivent pas être traitées (donc également communiquées) d'une manière à laquelle la personne concernée ne pourrait adhérer.

Par le passé, l'établissement financier avait toujours assuré à ses clients que leurs données personnelles n'étaient accessibles qu'aux collaborateurs responsables, nominalement connus, du centre de consultation financière dans la ville A. La base d'une *relation de confiance* entre le client et son conseiller financier était ainsi créée. Elle permettait au client de communiquer à son conseiller certaines données sensibles sur sa personne. Cette assurance peut donc être considérée comme élément essentiel subjectif du contrat et exclut une communication du dossier du client à des personnes extérieures à cette relation de confiance.

La fusion des deux centres de consultation financière modifiait inévitablement non seulement le cercle des personnes traitant les données, mais aussi les modalités de traitement convenues à l'origine et, par-là, la relation de confiance en tant que telle. Eu égard à la relation de confiance déjà existante et du contenu confidentiel des dossiers des clients, le principe de transparence requiert que les personnes concernées soient informées de la transmission de leurs données au nouveau centre de consultation financière (et de ce fait à de nouveaux collaborateurs). C'est le seul moyen de garantir que le client puisse donner son consentement.

Ce consentement fournit donc le motif justificatif requis par l'art. 12, al. 2, lettre c LPD. Il convient à cet égard de considérer ce qui suit: plus les données sont sensibles, plus les exigences posées à la transparence du consentement sont élevées. Donc, les clients doivent être informés de manière *exhaustive* du fait que leurs données seront communiquées à un nouveau centre de consultation financière. Dans pareil cas, il ne faut pas que le consentement de chaque personne concernée soit donné de manière tacite, mais il doit être expressément recueilli et - du fait qu'il s'agit de données personnelles particulièrement sensibles - doit avoir lieu par écrit.

Du point de vue du droit de la protection des données, les personnes concernées ne sont en mesure de donner un consentement valide que si elles possèdent suffisamment d'informations sur le but futur du traitement, sur la portée de la communication des données et sur la personne à qui sera confiée le dossier.

8.4 Publicité illicite par courrier électronique (spam)

Face à l'accroissement rapide du nombre de messages publicitaires non sollicités, la situation de droit a évolué pratiquement dans le monde entier. En Suisse, la tendance qui se dessine est de voir le principe du «opt-out» remplacé par celui du «opt-in», lequel est en vigueur dans l'Union européenne depuis octobre dernier.

Dans notre précédent rapport d'activités (cf. notre 10ème Rapport d'activités 2002/2003, paragraphe 6), nous avons exposé le sujet du spam sur le fond et décrit quelles conditions doivent être remplies pour que l'envoi de messages publicitaires non sollicités soit licite. Selon la situation juridique actuelle en Suisse, ces conditions se résument comme suit: premièrement, seules des adresses collectées de manière licite peuvent être utilisées et deuxièmement, un moyen simple doit être proposé aux destinataires pour leur permettre d'exercer leur droit d'opposition (droit à un «opt-out»).

Suivant en cela l'évolution dans l'Union européenne, on peut observer en Suisse une tendance vers des conditions plus strictes quant à la licéité. Les Etats de l'Union

européenne appliquent depuis fin octobre 2003 le principe de l'«opt-in», c'est-à-dire que l'envoi de messages publicitaires n'est désormais permis que si le destinataire y a expressément consenti au préalable ou une relation d'affaires existe déjà entre le destinataire et l'expéditeur. Même si la formulation exacte qui entrera dans la législation suisse n'est pas encore claire, l'intention semble nettement exprimée d'introduire chez nous aussi le principe de l'«opt-in». C'est du moins ce qui figure dans le message relatif à la modification de la loi sur les télécommunications (LTC, FF 2003 7260). La formulation dans le projet de l'article correspondant qui doit être ajouté à la loi fédérale contre la concurrence déloyale (LCD) ne correspond cependant pas à cette intention. Selon les termes de ce dernier, fait de la publicité déloyale celui qui envoie, par voie de télécommunication, de la publicité de masse «et omet de requérir préalablement le consentement des clients, de mentionner correctement l'émetteur ou de faire état de la possibilité de s'opposer gratuitement à cette publicité» (tiré du projet d'art. 3, lettre o LCD). De ce fait, la simple mention d'une possibilité de s'opposer constituerait une alternative au consentement préalable des destinataires, ce qui remettrait en vigueur le principe de l'«opt-out».

Au-delà, deux points sont essentiels dans le cadre de la révision actuelle de la LTC. Un premier aspect important de la révision prévue de la LCD est le fait qu'une violation de la règle de comportement par les annonceurs sera dorénavant passible d'une peine. D'autre part, dans le cadre de la même révision de loi, les fournisseurs de services de télécommunication auront l'obligation de combattre la publicité de masse déloyale. Cette disposition aura sans doute l'effet le plus significatif dans les situations où les fournisseurs d'accès peuvent eux-mêmes tirer profit du fait que de la publicité est adressée à leurs utilisateurs. A ce sujet, on pensera en premier lieu au domaine encore peu développé du «Location Based Advertising», qui n'est absolument pas réalisable sans les fournisseurs.

La recommandation mentionnée dans notre 10ème Rapport d'activités concernant l'annonceur domicilié à Zurich est actuellement pendante auprès de la CFPD. En relation avec cette recommandation, un point litigieux est l'effort que l'annonceur peut exiger des personnes concernées dans l'exercice de leurs droits d'«opt-out». L'annonceur, selon ses dires, offre les possibilités du courrier postal et de la télécopie, alors que le PFPD demande une possibilité de contestation par le même moyen de communication.

9. Finances

9.1 Questions concernant la protection des données lors de l'exercice des droits d'actionnaires

Il nous a été demandé d'examiner sous l'angle de la protection des données le problème de l'enregistrement du comportement de vote des actionnaires lors de l'assemblée générale d'une société, notamment lorsque les personnes concernées sont en même temps salariés de l'entreprise en question. Il apparaît que les actionnaires ne peuvent prétendre au vote secret et que certains traitements de données personnelles sont nécessaires en relation avec l'exercice des droits d'actionnaires conformément aux dispositions du droit de la société anonyme. Par contre, une utilisation de données sur le comportement de vote en relation avec le rapport de travail se justifie tout au plus au niveau des membres de la direction. Globalement, il convient d'exiger surtout que les traitements effectués soient placés sous le signe de la transparence.

Le droit de la société anonyme prévoit un certain nombre de droits de participation pour les actionnaires. En font notamment partie le droit de vote lors de l'assemblée générale ainsi que le droit de porter certains objets à l'ordre du jour sous certaines conditions. Il est examiné ci-dessous à propos de ces droits de participation dans quelle mesure ils peuvent requérir et justifier un traitement de données personnelles des actionnaires.

Enregistrement du comportement de vote

Si le comportement de vote est noté de telle sorte qu'il est possible de déterminer la manière dont un actionnaire a voté, nous sommes alors en présence de données qui se rapportent à un actionnaire déterminé ou pour le moins déterminable. Il s'agit donc de données personnelles conformément à la LPD.

Le droit de la société anonyme ne s'exprime pas sur la forme dont le vote doit avoir lieu durant l'assemblée générale. Le vote à main levée ainsi que le vote par écrit sont tous deux courants. Dans la mesure où les statuts ne renferment pas de règlement précis à ce propos, le conseil d'administration détermine le mode de votation car c'est lui qui est au premier chef responsable de la tenue de l'assemblée générale. On peut également imaginer que l'assemblée générale elle-même décide si elle vote à main levée ou à vote secret par écrit dans un cas déterminé. Dans la mesure où les statuts ne le prévoient pas, l'actionnaire ne peut prétendre à un vote écrit et absolument secret (c'est-à-dire non seulement vis-à-vis de l'actionnariat, mais aussi vis-à-vis du conseil d'administration) en vertu du droit de la société anonyme.

A titre de motif justificatif de l'enregistrement du comportement de vote, l'assemblée générale peut notamment faire valoir qu'il doit lui être possible, en cas d'action révocatoire, d'action concernant le droit de vote ou encore dans le cadre d'un procès, de prouver comment l'actionnaire plaignant a voté. Selon la jurisprudence du Tribunal fédéral, seuls les actionnaires qui n'ont pas approuvé la décision contestée de l'assemblée générale sont en droit d'intenter une action.

Droit de faire inscrire un objet à l'ordre du jour

Les actionnaires qui représentent une certaine quantité de valeurs nominales peuvent demander qu'un objet soit mis à l'ordre du jour. Ils doivent prouver à la société que les quotas légaux ont été atteints. Cela requiert l'identification claire des actionnaires requérants. Cette preuve ne peut être apportée que si les actionnaires concernés se font reconnaître, en indiquant le capital qu'ils représentent, directement vis-à-vis de la société ou si une procuration écrite est donnée en faveur d'un mandataire. La procuration doit être présentée par ce mandataire à l'assemblée générale. La société a besoin des informations requises pour constater l'exercice légal du droit de faire inscrire un objet à l'ordre du jour. De ce fait, cette règle du droit de la société anonyme requiert obligatoirement le traitement de données personnelles.

Représentation du droit de vote

Le droit de la société anonyme autorise en principe l'actionnaire à se faire représenter à l'assemblée générale. Il connaît trois formes de représentation institutionnelle dans le cadre du droit de vote: le représentant membre d'un organe de la société, le représentant indépendant et le représentant dépositaire. Les représentants institutionnels sont tenus de communiquer à la société le nombre, le genre, la valeur nominale et les catégories d'actions qu'ils représentent. Ces informations doivent à nouveau être transmises par le président à l'assemblée des actionnaires présents et être consignées dans le procès-verbal de l'assemblée générale.

Le représentant doit donc apporter à l'égard de la société anonyme la preuve qu'un ou plusieurs actionnaires l'ont mandaté pour le ou les représenter à l'assemblée générale. Selon la doctrine actuelle, la simple forme écrite de la procuration est la condition de validité. Elle permet la légitimation incontestable du représentant à l'égard de la société et, le cas échéant, à l'égard d'autres participants à l'assemblée générale.

Le représentant institutionnel est légalement tenu de suivre les instructions de l'actionnaire. La doctrine dominante estime néanmoins que cette obligation concerne uniquement la relation entre le représentant et le représenté et que la société anonyme n'est pas tenue de surveiller le représentant dans son comportement de vote.

Pour l'entreprise, il est important de savoir uniquement dans la perspective d'un éventuel procès en révocation comment le représentant institutionnel a voté, mais pas de savoir quel actionnaire a donné quelles instructions. La mention d'instructions par l'actionnaire sur le document de procuration même ne semble pas absolument obligatoire sous l'angle du droit de la société anonyme. Rien ne s'oppose donc à ce que les instructions soient inscrites sur un formulaire séparé qui demeure en possession du représentant.

Par ailleurs, se pose la question de savoir si la société est habilitée à demander la publication des instructions écrites. Du point de vue de la protection des données, cela ne repose sur aucun motif justificatif. En outre, la société anonyme dans sa totalité n'a pas d'intérêts qui priment sur ceux de chaque actionnaire. Ce n'est que si l'actionnaire est prêt à publier volontairement des données que la société anonyme peut les collecter et les traiter.

Les actionnaires en tant qu'employés

Les obligations de l'employeur à propos du traitement des données personnelles de ses employés sont réglées par le droit du contrat de travail. Selon celui-ci, l'employeur ne peut traiter des données concernant l'employé que dans la mesure où ces données portent sur les aptitudes de celui-ci à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la LPD sont applicables.

En principe, le comportement de vote de l'actionnaire peut certes être enregistré lors de l'assemblée générale, ainsi que nous l'avons mentionné plus haut. Par contre, il est illicite pour des raisons relevant du droit de la protection des données d'utiliser des données concernant le comportement de vote en relation avec le rapport de travail lorsque l'employé est aussi actionnaire. Dans la perspective du principe de transparence posé par le droit de la protection des données, il serait donc judicieux que l'employeur soit tenu explicitement par contrat à ne pas traiter les données personnelles émanant du rapport d'actionnaire en relation avec le rapport de travail.

Cette constatation vaut en principe également pour les membres de la direction. Mais étant donné que tant leur comportement de vote que leur activité sur le lieu de travail déterminent de manière essentielle la politique d'entreprise de la société anonyme, un rapport étroit lie ces deux domaines dans cette catégorie d'employés. En outre, les actionnaires ont un intérêt supérieur à connaître le comportement de vote et de ce fait aussi la position des membres de la direction. Dans ces cas, l'utilisation des données sur le comportement de vote peut se justifier selon les circonstances. Il est également conseillé de prévoir ce traitement de données dans le contrat de travail.

Traitement de données respectueux du but poursuivi

Lorsqu'il s'agit de traitements de données nécessaires dans le cadre de l'exercice de ces droits, il convient toujours de tenir compte du fait que ces droits d'actionnaires découlent d'un rapport assimilable à un rapport contractuel intervenu sur une base volontaire. Les personnes concernées se soumettent à certaines règles de droits qui peuvent légitimer le traitement de leurs données personnelles.

En résumé, il convient de souligner que la saisie du comportement de vote (et d'autres données personnelles en rapport avec l'exercice des droits de participation en droit de la société anonyme) par la société anonyme est licite à condition qu'il y ait un motif justificatif. En général, celui-ci se trouvera dans une disposition du droit de la société anonyme. Le traitement des données doit ensuite être effectué dans le but qui avait été fixé, c'est-à-dire uniquement dans le but prévu par la loi. Une utilisation des données dans un autre but est impossible à moins qu'un nouveau motif justificatif n'apparaisse.

Cela peut être par exemple le cas de l'intérêt prépondérant des actionnaires à connaître le comportement de vote des membres de la direction ou du conseil d'administration. Il montre entre autres les stratégies de la politique d'entreprise et a une influence directe sur la marche future de la société anonyme.

Le conseil d'administration doit veiller à ce que les données personnelles notées lors de l'assemblée générale soient traitées en conformité avec les principes de la protection des données. Il doit prendre ou ordonner les mesures techniques et organisationnelles requises et édicter des instructions sur les autres modalités de traitement (autorisations d'accès, durée de conservation, etc.). Le principe de transparence requiert que les actionnaires soient informés sur ces traitements de données.

9.2 Adhésion à un organisme d'autorégulation

La question de savoir s'il est possible d'exiger la signature d'un document particulier ou d'une procuration lorsqu'un intermédiaire désire s'affilier à un organisme d'autorégulation selon la loi sur le blanchiment d'argent ne relève pas en premier lieu de la protection des données. La question qui doit plutôt être posée est de savoir si cette procédure est nécessaire pour l'accomplissement des devoirs selon la loi sur le blanchiment d'argent. L'organisme d'autorégulation pour sa part est soumis à la surveillance de l'autorité de contrôle pour la lutte contre le blanchiment d'argent qui dispose aussi des compétences techniques requises pour répondre à la question. Les personnes concernées sont libres de se soumettre à un autre organisme d'autorégulation ou à l'autorité de contrôle.

On nous a soumis la question de savoir s'il était possible d'exiger la signature du formulaire «Procuration relative à l'accomplissement des devoirs selon les art. 9 et 10 LBA» (LBA = loi fédérale sur la lutte contre le blanchiment d'argent dans le secteur financier). Il ne s'agit pas en premier lieu d'un problème relevant de la protection des données. Sur la base des traitements de données intervenant généralement en relation avec la LBA, le PFPD s'était permis les remarques suivantes:

Dans le cas présent, il s'agissait avant tout de savoir si l'octroi d'une procuration est nécessaire pour l'accomplissement des devoirs au sens de la LBA (obligation de communiquer et blocage des avoirs). Ceci ne ressort pas de la teneur des dispositions applicables (art. 9 et 10 LBA). D'un autre côté, un organisme d'autorégulation doit, aux termes de la LBA, veiller à ce que les intermédiaires financiers qui lui sont rattachés observent leurs devoirs conformément au deuxième chapitre de la LBA (dont notamment les art. 9 et 10). L'organisme d'autorégulation est pour sa part soumis à la surveillance de l'autorité de contrôle en matière de lutte contre le blanchiment d'argent. L'autorité de contrôle approuve aussi les règlements édictés par les organismes d'autorégulation. Pour cette raison, mais aussi parce que l'autorité de contrôle dispose des connaissances techniques requises concernant la LBA, nous avons prié la personne concernée d'adresser sa question directement à l'autorité de contrôle.

Nous avons fait remarquer à la personne concernée qu'elle était libre de se soumettre à un autre organisme d'autorégulation ou au contrôle direct des autorités (soit l'autorité de contrôle).

10. Statistique et recherche

10.1 Le rôle de la protection des données dans la statistique

Dans le cadre d'une demande de l'Office fédéral de la statistique, nous avons salué la volonté de cet office de se doter de principes de protection des données. Pour ce qui est du contenu des principes présentés, il nous semble qu'il y a encore à faire, principalement en ce qui concerne la clarté de la relation entre les traitements de données à des fins administratives et ceux à des fins statistiques.

Après l'adoption des principes de protection des données de l'Office fédéral de la statistique par sa direction, le conseiller à la protection des données de cet office nous a demandé notre avis. Nous avons salué aussi bien l'initiative en soi, que le fait que les principes aient été formulés en partie de manière très concrète et donc réalisable.

D'un autre côté, nous avons reproché que la relation entre les traitements de données à des fins administratives et ceux à des fins statistiques n'ait pas fait l'objet de réflexions concrètes, alors que cette relation est primordiale pour la protection des données en statistique. Au contraire, le document sur les principes de protection des données contient une formulation inquiétante à notre avis, selon laquelle les citoyens seraient de plus en plus disposés à accepter la liaison de données et leur utilisation multifonctionnelle à des fins statistiques et administratives si la protection des données est assurée. Du point de vue de la protection des données, ces deux genres de traitements de données sont complètement contraires et une mise au point de leur relation est à notre avis urgente pour la statistique, car nous observons de plus en plus, au cours de ces dernières années, que la statistique favorise l'accroissement et l'intensification des traitements de données à des fins administratives. Citons-en deux exemples: Depuis l'introduction du registre fédéral des bâtiments et des logements, les autorités de contrôle des habitants ont l'obligation d'attribuer chaque habitant à un numéro de bâtiment et de logement. Prenons comme deuxième exemple ce que l'on appelle l'identificateur de personnes fédéral qui permet de faciliter la mise en relation de registres administratifs, aussi et justement pour le domaine administratif. Il est manifeste qu'une telle possibilité de mise en relation entraîne des risques plus importants pour les droits de la personnalité que de simples traitements statistiques. Il est toutefois un fait que, sous la contrainte de temps que représente le recensement 2010, une infrastructure est mise en place qui pourrait, par exemple, permettre des investigations par recoupements à grande échelle. Qu'il soit aujourd'hui question d'«identificateurs de personnes sectoriels coordonnés» n'y change au fond rien non plus. Plutôt qu'un élément de mise en relation sans finalité claire, on en crée ainsi

simplement plusieurs sans définir au préalable leurs objectifs de manière suffisamment précise.

Eu égard à de tels effets sur le domaine administratif, nous avons suggéré que l'Office fédéral de la statistique présente un concept sur la manière d'empêcher à l'avenir que l'activité administrative ne soit influencée par la statistique.

10.2 Projets de recherche et études cliniques: conséquences d'un consentement révoqué

La participation à un projet de recherche ou à des études cliniques est toujours volontaire et peut être révoquée en tout temps. Lorsqu'un participant révoque son consentement, il peut admettre que ses données seront détruites, sauf s'il a expressément donné son accord à la réutilisation des données. Si la question n'a pas été réglée, on ne peut pas présumer que le participant serait d'accord avec la réutilisation de ses données. Comme en cas de révocation du consentement, les données ne sont plus disponibles pour le projet de recherche ou pour l'étude, il est conseillé d'anonymiser les données dès que possible. Du fait qu'il n'est plus possible de les attribuer, les données anonymisées ne constituent plus des données personnelles.

La participation à un projet de recherche ou à une étude est toujours volontaire. Un consentement à la participation peut être révoqué en tout temps sans indication du motif. Le consentement, donné normalement par écrit, n'est valable que si le participant a été suffisamment informé au préalable sur la finalité du projet ainsi que sur les traitements de données prévus. Dans la pratique, ceci est fait en remettant des notices d'information et en menant des entretiens. Nous avons été consultés par un institut sur les conséquences qu'aurait la révocation d'un tel consentement.

Le droit à l'autodétermination individuelle en matière d'information doit permettre au citoyen de disposer lui-même de ses données. Il lui permet de garder le contrôle sur le traitement de ses données. Ceci est également valable lorsqu'il donne son consentement au traitement de ses données. Outre le caractère volontaire, la révocabilité permanente est une exigence fondamentale des déclarations de consentement.

Pour qu'un consentement soit valable, la personne concernée doit pouvoir en saisir la portée (étendue et finalité), il est alors qualifié d'éclairé. Le respect du principe de transparence dans la formulation des clauses de consentement et des formulaires d'information est déterminant. La personne participant à une étude doit être pleinement informée sur la finalité et le déroulement de l'étude. De même, tous les traitements de données et dispositions de protection des données (transmission, stocka-

ge, destruction des données, protection contre l'accès par des tiers non autorisés, mesures de pseudonymisation et d'anonymisation éventuellement prévues etc.) doivent être expliqués. De plus, le caractère volontaire du consentement et la possibilité de révocation à tout moment doivent être expressément mentionnés.

Lorsque quelqu'un révoque son consentement à participer à une étude, il peut déduire que ses données seront détruites. Pour plus de sûreté, il est recommandé de demander une confirmation de la suppression des données.

Il va de soi que le participant peut en tout temps donner son accord à ce que ses données traitées dans le cadre de l'étude jusqu'au moment de la révocation puissent continuer d'être utilisées. Une clause réglant ce point devrait figurer dans la déclaration de consentement. Se fondant sur son droit à l'autodétermination individuelle en matière d'information, il peut également en tout temps révoquer cet accord. Si la question n'est pas réglée, il n'est pas possible de déduire sans autre que les données peuvent continuer d'être utilisées. Lorsque les données ont été anonymisées, il n'y a aucun problème. Ceci est le cas lorsque toutes les caractéristiques qui permettent une identification de la personne ont été supprimées (cf. notre 3ème Rapport d'activités 1995/1996, paragraphe I 9.3). Le participant ne peut pas exiger la suppression de données qui ne se rapportent plus à des personnes identifiables.

Si les données ont été simplement pseudonymisées, les personnes qui ont accès à la table de correspondance contenant les fonctions d'attribution peuvent en tout temps les retransformer en données personnelles. Des données pseudonymisées peuvent être anonymisées en effaçant les fonctions d'attribution. Si un participant révoque sa participation à l'étude, ses données pseudonymisées peuvent être traitées comme suit: destruction de la seule fonction d'attribution et ainsi les données restent utilisables pour l'étude sous forme anonyme ou destruction de la fonction d'attribution et des données correspondantes. Dans l'intérêt de l'étude ou du projet de recherche, cette dernière solution ne devrait être appliquée que sur demande expresse de la personne concernée, puisque les données seraient alors perdues pour l'étude ou le projet de recherche. Ce risque peut être minimisé dans la pratique en rendant les données complètement anonymes dès que possible ou - lorsqu'une attribution doit encore être possible, mais pas nécessairement en relation avec une personne déterminée - en détruisant le pseudonyme et en le remplaçant par une identification sans fonction d'attribution.

Finalement, il reste à mentionner que tant que des données concernant une personne déterminée sont traitées dans le cadre d'une étude ou d'un projet de recherche, le participant jouit aussi en tout temps du droit d'accès que lui confère la LPD.

10.3 Indication de données médicales dans un questionnaire statistique

Des groupes de travail réunissant des fournisseurs de prestations dans le domaine de la santé collectent des données qui permettent aux personnes intéressées de comparer les prestations fournies. La vérification du projet de l'ASF (Groupe de travail des cliniques gynécologiques et obstétriques de Suisse) a, outre les problèmes «classiques» de la protection des données, soulevé aussi des interrogations reposant en majeure partie sur des malentendus dans la manière de traiter les questions de protection des données.

Sur l'indication que nous avons reçue d'un hôpital, nous avons analysé la collecte de données de l'ASF. Nous avons constaté que des données personnelles ainsi que des données médicales et statistiques ont été saisies sur un même formulaire. Transmises à un autre service, ces données ont été traitées à des fins de statistique et de contrôle de qualité. La méthode de collecte est comparable avec le système décrit dans notre 9ème Rapport d'activités 2001/2002 au paragraphe 5.1.6. Pour cette raison, nous renonçons à l'aborder plus en détail ici.

Il nous paraît cependant intéressant de mentionner trois questions soulevées lors de l'examen du projet de l'ASF.

La première question qui se pose est de savoir si l'accord écrit des médecins-chefs suffit pour permettre la communication de données médicales à des tiers. La réponse est clairement non. L'accord écrit n'est pas une légitimation suffisante pour une communication non anonymisée de données sensibles à des tiers.

Il y a lieu par ailleurs de déterminer s'il suffit que le traitement des données médicales se fasse de manière soigneuse ou s'il faut plus. Cela dépend de la façon dont se conçoit ce soin. Il ne pourra pas remplacer une procédure parfaitement vérifiée et réglée pour l'utilisation de données concernant le patient. Ce n'est qu'après une analyse approfondie des bases légales, des besoins et de la finalité du traitement des données qu'il sera possible d'ébaucher une solution, dont l'introduction et l'application devraient ensuite s'effectuer avec soin.

Il reste finalement la question de savoir pourquoi une période de 20 ans sans incident relevant de la protection des données ne peut pas valoir comme preuve que la protection des données est respectée. On ne peut que se réjouir qu'une entreprise ne déplore aucun incident touchant à la protection des données pendant une période de 20 ans. La protection des données est souvent confondue avec la sécurité des données ou la sécurité informatique. Même si des données, qui sont transportées sur des réseaux bien protégés et stockées et traitées dans des systèmes hautement sécuri-

sés, n'ont jamais été perdues ou manipulées par un pirate informatique, il peut exister une violation de la protection des données. Par exemple lorsque le traitement des données n'est pas licite ou proportionnel et ne respecte pas le principe de la bonne foi ou lorsque les données personnelles ne sont plus traitées aux fins initialement prévues.

11. International

11.1 Conseil de l'Europe

11.1.1 Projet de protocole sur la génétique humaine

Le Conseil de l'Europe a soumis pour avis la première partie du protocole aux milieux concernés. Les résultats de la procédure de consultation sont disponibles. Les membres du groupe de travail ad hoc ont eu à nouveau l'occasion de se prononcer à ce sujet.

Le protocole sur la génétique humaine est l'un des protocoles additionnels à la Convention du Conseil de l'Europe sur les droits de l'Homme et la biomédecine (Convention d'Oviedo). Ce protocole a pour but de réglementer les analyses génétiques dans le domaine médical ainsi que dans le domaine du travail et des assurances (pour plus de détails à ce sujet, cf. notre 10ème Rapport d'activités 2002/2003, paragraphe 11.1.4). Il devrait entre autres permettre d'éviter les discriminations fondées sur le patrimoine génétique.

La première partie du protocole concerne le domaine médical. Les Etats membres ainsi que d'autres milieux concernés se sont exprimés à son sujet. Ensuite, le groupe de travail a eu encore la possibilité de prendre position sur les résultats de la consultation.

Il est important, du point de vue de la protection des données, que l'actuelle législation en matière de protection des données du Conseil de l'Europe soit prise en considération dans le protocole. Mentionnons en particulier diverses recommandations du Conseil de l'Europe. Ces recommandations ont pour contenu le traitement des données médicales en général et les analyses génétiques en particulier.

Le traitement de données génétiques pose surtout des exigences très hautes en matière de sécurité des données et de confidentialité. Pour cette raison, le protocole doit établir les conditions dans lesquelles le matériel biologique et les informations qui s'y rapportent sont converties en données anonymisées ou pseudonymisées.

Il est prévu que la première partie du protocole sera une fois encore remaniée au sein de divers organes du Conseil de l'Europe. Au cours de l'année écoulée, le groupe de travail s'est par ailleurs rencontré pour la dixième fois à Strasbourg. Cette rencontre avait pour but l'élaboration de la seconde partie du protocole devant réglementer les analyses génétiques dans le domaine du travail.

11.1.2 Travaux du CJPD: carte à puce et biométrie

Le Groupe de projet sur la protection des données (CJPD) s'est réuni pour la dernière fois du 24 au 27 novembre 2003. Il a adopté un projet de principes directeurs sur la protection des données à l'égard des cartes à puce.

Lors de sa 41ème et dernière réunion, le CJPD a adopté un projet de principes directeurs sur la protection des données personnelles à l'égard des cartes à puce. Ce texte énonce les principes à prendre en considération pour améliorer la protection des données lors de l'utilisation de cette technologie. Les principes directeurs élaborés par le comité ne prétendent pas apporter une solution exhaustive à tous les problèmes de protection des données liés à l'utilisation des cartes à puce. En effet, ces dernières sont toujours intégrées dans un système d'information plus vaste. L'effectivité de la protection dépend de nombreux facteurs et circonstances, ainsi que du comportement des personnes impliquées par ce système. Les principes directeurs définissent les règles de base à respecter lors de la collecte et du traitement de données personnelles au moyen de cartes à puce. Ils mettent en particulier l'accent sur les principes de finalité, de proportionnalité et de transparence (devoir d'information à l'égard des utilisateurs). Le CJPD a également examiné, en première lecture, un projet de principes directeurs sur la protection des données à l'égard de l'utilisation des données biométriques. Toutefois, après plus de 20 ans d'activités, le Conseil de l'Europe a décidé, pour des raisons budgétaires, de mettre un terme aux activités du CJPD. Les travaux du CJPD, notamment sur la biométrie seront repris par le Comité consultatif (T-PD). Les experts ont pris note de la suppression de ce comité. Ils ont regretté la fin brutale d'un comité qui a largement contribué au développement du droit de la protection des données en Europe et qui était un laboratoire pour les Etats qui n'avaient pas de législation de protection des données. Les experts ont ainsi invité le Conseil de l'Europe à étudier la manière de garantir la participation des Etats n'ayant pas ratifié la Convention 108 aux travaux du T-PD qui réunit les parties à la Convention.

11.1.3 Travaux du T-PD: programme de travail et flux transfrontières de données

Le Comité consultatif de la Convention 108 (T-PD) a tenu sa 19ème réunion du 27 au 29 novembre 2003. Il a adopté son programme de travail et ses priorités pour les années à venir. Il a en outre examiné un projet d'avis concernant le transfert régulier et massif de données à caractère personnel vers un Etat tiers n'offrant pas un niveau de protection adéquat.

Sous présidence suisse, le T-PD a adopté son programme de travail et ses priorités pour les années à venir. Le T-PD abordera en priorité la biométrie et finalisera le projet préparé par le CJPD. Il se penchera ensuite sur les droits des personnes concernées, en élaborant notamment un guide à l'intention des personnes concernées. Ce guide devrait rappeler le cadre juridique de la protection des données, énoncer les droits et les devoirs des personnes concernées et la manière de faire valoir leurs droits et leurs prétentions dans l'ensemble des Etats parties à la Convention. Il s'attachera à l'examen du niveau de protection adéquat des Etats tiers, notamment en élaborant des avis. Enfin, il examinera l'application des principes de protection des données à l'Internet.

Le T-PD a ensuite étudié un projet d'avis relatif au transfert régulier et massif de données à caractère personnel vers un Etat tiers n'offrant pas un niveau de protection adéquat. Cet avis devait en particulier rappeler le cadre minimal à respecter lorsqu'un responsable de traitement est tenu de transférer des données vers un Etat tiers n'assurant pas un niveau de protection adéquat en vertu d'obligations imposées par cet Etat tiers. Toutefois le comité n'a pas été en mesure de dégager un consensus sur ce projet et a convenu de réexaminer la question ultérieurement. Le T-PD a en outre modifié son règlement intérieur notamment pour améliorer son fonctionnement et sa prise de décision. Il a réélu Madame W. Kotschy de l'Autriche en qualité de Commissaire à la protection des données du Conseil de l'Europe.

11.2 Union européenne

11.2.1 Groupe de travail européen sur le traitement des plaintes et les échanges d'informations

Ce groupe de travail auquel nous participons a mis l'accent lors de sa réunion d'octobre 2003 sur l'examen de cas concrets afin de comparer les différentes méthodes de surveillance appliquées par les autorités de contrôle de protection des données lors de l'instruction de plaintes. Le groupe de travail a également porté une attention particulière à son élargissement en relevant la nécessité de revoir son mode de fonctionnement.

Sur la base du mandat attribué par la Conférence européenne des Commissaires à la protection des données, le groupe de travail européen «traitement des plaintes et échanges d'informations» (Complaints handling Workshop) s'est réuni les 23 et 24 octobre 2003 à Rome. Nous avons participé aux travaux de ce groupe dont le but est d'analyser les différentes méthodes de traitement des plaintes déposées auprès des autorités de protection des données et de favoriser la coopération entre ces dernières.

Lors de cette réunion, le groupe de travail a poursuivi les études entamées au cours des précédentes réunions. Alors que celles-ci étaient consacrées aux méthodes de contrôle utilisées par les autorités de protection des données en fonction de leurs compétences légales respectives, la réunion de Rome a permis de concrétiser ces méthodes par l'examen de cas concrets. Ont ainsi été analysés différents cas touchant notamment aux traitements de données biométriques, aux flux transfrontières, à la vidéosurveillance sur le lieu de travail ou à la conservation de données par des agences de renseignements de crédits. Cette démarche a mis en évidence non seulement les avantages ou désavantages des méthodes de surveillance utilisées ainsi que les différences de résultat obtenu, mais également l'importance de clarifier dans chaque cas d'espèce si l'autorité de protection des données agit dans le cadre de ses compétences de surveillance ou de conseil.

Face à ces approches et résultats différents dans le traitement des plaintes, le groupe de travail a rappelé l'importance des échanges d'informations et d'expériences entre autorités de protection des données. Il a ainsi réaffirmé le rôle fondamental du système informatique CIRCA (Communication & Information Resource Centre Administrator). Ce système extranet sécurisé lié au programme IDA (Interexchange of Data between Administrations) de la Commission européenne, offre une plate-forme d'échange d'informations concernant des résultats de contrôles effectués ainsi que

des conseils ou des solutions trouvées à des problèmes similaires de protection des données.

Enfin, le groupe de travail a porté une attention particulière à l'augmentation de ses membres. Composé au départ d'une vingtaine de participants représentant l'Union européenne et certains Etats ayant un niveau de protection adéquat tel que la Suisse, le groupe s'est fortement agrandi avec l'arrivée de nouveaux participants (Tchéquie, Slovaquie, Slovénie, Lituanie, Pologne, etc.). Approchant la cinquantaine de participants, le groupe de travail a relevé la nécessité de revoir son mode de fonctionnement. Tout en souhaitant conserver un caractère informel favorisant les échanges d'expériences, le groupe estime nécessaire de mieux organiser les différentes interventions des participants et de mieux coordonner les choix des thèmes des réunions, notamment par rapport aux travaux en cours du Groupe de l'article 29 de l'Union européenne. Plusieurs intervenants ont proposé la création d'un comité de programme chargé du suivi et de la gestion des thèmes à traiter.

Le groupe de travail va poursuivre ses activités avec pour objectif l'amélioration de la collaboration entre autorités nationales de contrôle dans le cadre de l'examen des plaintes qu'elles traitent et des inspections ou contrôles qu'elles effectuent. En outre, des réflexions sur le mode de fonctionnement du groupe de travail seront présentées à la prochaine Conférence européenne des Commissaires à la protection des données qui se tiendra à Rotterdam en avril 2004.

11.2.2 Conférence européenne des commissaires à la protection des données

Les commissaires européens à la protection des données se sont réunis les 3 et 4 avril 2003 à Séville. Nous y avons participé en tant qu'observateur. Les commissaires ont accueilli favorablement la proposition suisse d'ouvrir la conférence à toutes les autorités de protection des données des Etats ayant ratifié la Convention 108.

La Conférence européenne des commissaires à la protection des données réunit les commissaires des pays membres de l'Union européenne. Les pays membres de l'Espace économique européen, les pays candidats à l'adhésion à l'Union européenne ainsi que la Suisse sont invités à y participer en tant qu'observateurs. Les représentants de la Commission européenne, du Conseil de l'Europe et de l'autorité de surveillance en matière de protection des données d'Europol ont également pris part aux travaux.

Cette année, la Conférence était présidée par l'autorité espagnole de protection des données et s'est déroulée à Séville. La Conférence a abordé des questions complexes et liées à l'actualité. Elle a ainsi permis de s'interroger sur le rôle que les autorités de surveillance en matière de protection des données doivent jouer en Europe, de faire un premier bilan de l'application de la directive européenne et d'examiner l'état de la protection des données dans les Etats candidats à l'adhésion à l'Union européenne. Les commissaires ont également débattu de la protection des données dans le domaine des télécommunications, du e-marketing et des problèmes liés aux flux transfrontières de données. Les commissaires ont ainsi exprimé la nécessité de réévaluer le rôle et les objectifs des autorités nationales de surveillance dans un monde où l'usage des technologies de l'information revêt une dimension universelle et dans lequel le droit à la protection des données est plus que jamais appelé à être un élément déterminant de la qualité de vie. Ils ont en particulier mis l'accent sur la nécessité de renforcer la collaboration internationale, notamment eu égard aux flux transfrontières de données. Ils ont rappelé que les fournisseurs de services dans le domaine des télécommunications devaient mettre en place les mécanismes nécessaires pour protéger les données personnelles des utilisateurs. La Conférence a également permis de faire le point sur les mesures prises suite aux attentats de septembre 2001. Les commissaires ont ainsi insisté sur l'équilibre à maintenir entre les besoins de la sécurité et de la lutte contre le terrorisme et l'indispensable garantie du respect de la vie privée. Cet équilibre ne peut se faire au détriment de la protection des données. Enfin, nous avons proposé que la Conférence réfléchisse sur son avenir et évolue vers une conférence regroupant l'ensemble des autorités de surveillance des Etats parties à la Convention du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La Conférence a accueilli favorablement cette proposition.

11.3 OCDE

11.3.1 Groupe de travail sur la sécurité de l'information et la protection de la sphère privée (WPISP)

Au cours de l'année écoulée, le groupe de travail s'est réuni à deux reprises. Les discussions ont porté sur la mise en œuvre des nouvelles directives concernant la sécurité de l'information, sur l'authentification électronique, sur le rapport concernant les applications de la biométrie et, enfin, sur le problème des spams. Pour la deuxième année consécutive, la mise au point d'une structure globale de la sécurité a constitué le point fort des travaux du groupe de travail. Par ailleurs, une conférence spéciale sur la sécurité globale s'est tenue à Oslo.

Les nouvelles directives de l'OCDE sur la sécurité ont été également reprises par l'ONU. Mais, malgré leur publication, l'état de la mise en œuvre de ces directives dans les Etats membres n'est pas satisfaisant. Il convient à cet endroit de souligner à quel point il est important de promouvoir la confiance de la population à propos de la sécurité. Ce n'est pas à l'utilisateur de rechercher une solution en matière de sécurité et de protection des données. Il est donc demandé aux entreprises d'intégrer déjà les mesures de sécurité et de protection des données au niveau du développement des logiciels et matériels informatiques.

En matière d'authentification électronique et de signature digitale, le groupe de travail a procédé à une analyse de la situation actuelle dans les Etats membres. Il leur recommande d'éviter les barrières de réglementation touchant la reconnaissance internationale des signatures digitales. Les travaux dans ce domaine doivent être coordonnés de manière plus étroite avec d'autres organisations internationales.

Le rapport sur les applications de la biométrie a été publié. Les risques pour la sphère privée et la sécurité en constitue le point fort, notamment les problèmes posés par l'identification (identity thief). Il présente en outre les applications techniques déjà disponibles de la biométrie et souligne la nécessité de définir des normes internationales.

Par ailleurs, le groupe de travail a élaboré une étude de base sur les spams. Cette étude servira de fondement pour les travaux futurs dans ce domaine.

Pour la deuxième année consécutive, la sécurité globale a été au cœur des activités du groupe de travail. Outre la conférence d'Oslo spécialement dédiée à la sécurité globale, le groupe de travail s'est penché sur la sécurité des transports internatio-

naux. Une séance ad hoc a été organisée à ce propos les 26 et 27 septembre 2003 à Londres. Les résultats de cette séance ont été présentés au groupe de travail WPISP. En résumé, les systèmes d'information existants doivent être exploités au maximum et reliés en eux; le volume des données doit être limité aux données lisibles par machine figurant dans les documents d'identité. Quelques Etats ont proposé d'établir une banque de données centrale, notamment pour les pays qui ne peuvent assumer financièrement leur propre banque de données. Mais le relevé de données supplémentaires dépend aussi de l'existence de traités bilatéraux. En définitive, il a été convenu de désigner un service de contrôle reconnu au niveau international pour la protection des donnés et la sécurité. Le groupe de travail WPISP a fait part à ce propos de l'intention d'élaborer un rapport pour que l'on puisse décider s'il faut éventuellement publier des recommandations de l'OCDE en matière de sécurité des transports. La majorité des Etats membres participants reconnaissent les risques liés à une action rapide en la matière et sont d'avis qu'il faudra ultérieurement décider si le groupe d'experts sur la sécurité de l'information et la protection de la sphère privée doit poursuivre les travaux dans ce domaine ou si une autre organisation serait plus adaptée pour cela (IATA, OACI).

La conférence sur la sécurité globale organisée les 13 et 14 octobre 2003 à Oslo a permis d'aborder divers thèmes. La problématique du développement d'une structure globale de la sécurité ne peut être résolue exclusivement par le dialogue entre les autorités et l'économie. Les citoyens doivent être intégrés à ce dialogue. Parallèlement, la réflexion sur la sécurité doit aussi tenir compte des principes de l'éthique et de la démocratie. En effet, l'appréciation entre les besoins de la sécurité et les principes de la démocratie laisse une marge de manœuvre très étroite. La limitation des droits démocratiques - dans la mesure où elle est effectivement nécessaire - doit donc absolument être précédée d'une analyse des enjeux socio-politiques.

Cette conférence a permis de mettre en lumière le fait que la protection de la sphère privée n'est pas suffisamment prise en compte dans le débat actuel sur la sécurité au sein de l'OCDE. Bien que la nécessité de mesures de sécurité demeure incontestée, surtout quant à la protection des systèmes d'information, elles ne doivent pas outrepasser le cadre légal des surveillances étatiques.

11.4 Autres thèmes

11.4.1 Conférence internationale des commissaires à la protection des données

La XXVème Conférence internationale des commissaires à la protection des données s'est déroulée à Sydney du 9 au 11 septembre 2003. Elle réunissait des délégations provenant de 35 Etats et quatre continents. La Conférence a mis l'accent sur les aspects pratiques de la protection des données et leurs conséquences pour l'individu, les administrations et les entreprises. Elle a permis l'adoption de cinq résolutions.

La 1ère partie de la Conférence était ouverte et réunissait au côté des commissaires à la protection des données, des représentants de l'industrie, des services, des administrations publiques, des consommateurs, de la recherche et du monde académique. La Conférence a mis l'accent sur des aspects pratiques liés à l'application des exigences de la protection des données (voir http://www.privacyconference2003.org/program.asp). Elle a permis de confronter des approches différentes entre des cultures et des systèmes juridiques divers. Dans un monde globalisé et interdépendant, elle a permis de mettre en évidence la difficulté d'une approche commune de la protection des données et pose de manière accrue la question de la nécessaire reconnaissance du caractère universel des principes de la protection des données tels qu'ils découlent des lignes directrices de l'OCDE ou de la Convention du Conseil de l'Europe. Une approche flexible et dynamique de la protection des données est certes indispensable pour assurer l'effectivité de la protection des données. Cela implique néanmoins le respect de principes de base. Ces principes ne peuvent être remis en question sans risquer de toucher non seulement au fondement des droits et des libertés individuels, mais aussi au caractère démocratique de nos sociétés. Ce respect est d'autant plus nécessaire que partout dans le monde, nous assistons à un accroissement des mesures de surveillance des individus, notamment dans le cadre de la lutte contre le terrorisme. Or, la protection des données fait partie intégrante d'une politique de sécurité. La Conférence est également préoccupée du développement des technologies de l'information et des risques qu'elles génèrent pour les droits et les libertés individuels. Aujourd'hui nous sommes confrontés à des réseaux qui lient différentes technologies et permettent de gérer des données de plus en plus nombreuses, voire de suivre l'individu dans tous ses agissements. Au travers de projets concrets, elle a également constaté que la technologie pouvait être utilisée conformément aux exigences de la protection des données. Enfin, la Conférence a souligné les efforts de nombreuses entreprises pour développer des règles de protection

des données (code de déontologie, règlement interne). Elle a pris positivement connaissance de leur souhait d'une plus grande harmonisation des dispositions et des pratiques de protection des données.

La 2e partie de la Conférence était réservée aux Commissaires à la protection des données. Elle a permis un échange de vue sur les développements majeurs intervenus depuis 2002. Les Commissaires ont en outre adopté, à l'unanimité, cinq résolutions (http://www.privacyconference2003.org/commissioners.asp). La première résolution concerne l'amélioration de la communication des pratiques relatives à la protection des données. Elle attire l'attention des responsables de traitement sur l'importance de l'information à fournir aux personnes concernées. Elle propose une marche à suivre en matière d'information et préconise en particulier de recourir à des formats succincts et standardisés. Cette résolution, proposée par l'Australie, a été préparée en étroite collaboration avec des représentants des responsables de traitement et des consommateurs. La deuxième résolution préparée par la Nouvelle-Zélande a trait à la protection des données et aux organisations internationales. Elle invite les organisations internationales notamment à se conformer à des principes compatibles avec les principaux instruments internationaux qui touchent à la protection des données. Une troisième résolution présentée par l'Allemagne porte sur la mise à jour automatisée des logiciels. Elle demande aux fournisseurs de logiciel de mettre en place des procédures qui respectent les droits des personnes concernées. En particulier, la mise à jour doit se faire de manière transparente et avec le consentement des personnes concernées. La quatrième résolution concerne le transfert des données des passagers. Elle a été présentée par la Suisse et demande en particulier que «lorsqu'un transfert international et régulier de données personnelles s'avère nécessaire, il devrait intervenir dans un cadre prenant en compte la protection des données, par exemple sur le fondement d'un accord international fixant les exigences adéquates de protection des données…» Enfin, l'Allemagne a proposé une résolution sur l'identification par radiofréquence (RFID). Cette résolution invite à tenir compte des principes de la protection des données lors du recours à cette technologie qui peut être particulièrement invasive.

12. Le Préposé fédéral à la protection des données

12.1 Réorganisation et réorientation des activités

Comme annoncé lors de la présentation du 10ème Rapport d'activités, nous avons réorienté nos activités et procédé à une restructuration de notre secrétariat. L'objectif poursuivi est un rééquilibrage entre les tâches de conseil et les tâches de surveillance. Ce rééquilibrage doit permettre une approche plus «proactive» de la protection des données et dégager des capacités pour les activités de surveillance.

Depuis l'entrée en vigueur de la LPD, le 1er juillet 1993, le monde s'est profondément modifié. Le domaine de la protection des données a été en particulier touché par la révolution électronique qui nous a propulsés dans un monde virtuel tout en augmentant sensiblement les risques d'atteinte à la personnalité. Les risques d'atteinte à la vie privée des personnes englobent tous les domaines d'activités de la société. La globalisation de la société et des échanges d'informations entraîne un éclatement et une dispersion croissante des traitements de données personnelles. Cette situation génère d'une part un risque d'affaiblissement de l'effectivité de la protection des données et d'autre part renforce l'importance et le caractère indispensable de la protection des données. Cela nécessite notamment une approche différente dans l'exercice des tâches du PFPD. Si durant les premières années d'activités, nous avons privilégié les activités de conseil et nous nous sommes efforcés de répondre à toutes les demandes adressées par les citoyennes et citoyens de ce pays, nous devons à l'avenir développer nos activités de surveillance, tout en maintenant nos activités de conseil. Pour faire mieux face aux défis de la société d'information, nous devons ainsi avoir une approche plus «proactive» des tâches légales qui nous sont conférées et ne pas nous limiter à vérifier le respect des dispositions légales. Notre action doit ainsi s'attacher à sensibiliser les individus et les responsables de traitement aux risques liés au traitement de données personnelles, notamment par:

- une politique d'information active,
- une évaluation des risques et l'élaboration d' «outils» permettant de réaliser les exigences de la protection des données et de diminuer les risques d'atteinte aux droits des personnes concernées,
- un encouragement des responsables de traitement à prendre leur responsabilité,
- un contrôle du respect des exigences légales.

Cette approche «proactive» de la protection des données implique en particulier:

- d'anticiper face aux nouvelles pratiques en procédant notamment à des études, en concertant les milieux concernés en vue de favoriser de meilleures pratiques qui pourront être transcrites dans des codes de conduite ou des règlements internes,
- d'anticiper face aux nouvelles technologies en adoptant des recommandations,
- d'anticiper en alertant les pouvoirs publics sur tel ou tel sujet d'ordre réglementaire ou législatif.

Afin d'assurer une meilleure effectivité de la protection des données, nous ne pouvons plus à l'avenir nous concentrer principalement sur le traitement de plaintes ou de demandes individuelles. Nous voulons mettre l'accent sur la prévention en axant nos actions sur l'étude des secteurs à risque avec pour objectif de définir les exigences de protection des données adaptées à ces secteurs et proposer des solutions pour leur permettre de continuer à fonctionner en tenant compte de ces exigences. Cette action préventive doit aussi s'attacher à définir et à promouvoir des outils permettant à l'individu de protéger sa vie privée. Elle doit encourager les responsables de traitement à prendre leur responsabilité et à recourir à des instruments comme l'audit en protection des données, les incitant à mettre leur organisation et leur processus de traitements en conformité avec les exigences légales. L'effectivité de la protection des données passe ensuite par des contrôles pour vérifier le respect des exigences légales et le cas échéant les abus devraient pouvoir être sanctionnés. Notre législation est à cet égard encore lacunaire et un renforcement des moyens de sanctions serait souhaitable (voir aussi notre 10ème Rapport d'activités 2002/2003, p. 17s.).

Nous souhaitons également renforcer notre politique d'information, non seulement pour attirer l'attention sur les risques, mais également pour communiquer les exigences de protection des données et les moyens de concrétiser ces exigences.

Une diminution de nos activités de conseil pour nous permettre de développer nos tâches de surveillance n'est pas sans conséquence pour les personnes concernées ou pour les responsables de traitement. Ainsi à l'avenir, nous ne serons plus en mesure de répondre systématiquement à toutes les demandes individuelles. Nous développerons par contre nos rubriques d'information pour permettre aux uns et aux autres de trouver des réponses aux questions les plus fréquentes.

En ce qui concerne l'administration fédérale, nous avons informé les départements et les offices fédéraux de nos nouvelles orientations. Nous avons en particulier attirer leur attention sur le fait que nous ne serons plus en mesure d'accompagner tous les projets, notamment en participant à des commissions ou des groupes de travail. En dehors des procédures de consultation pour des projets législatifs, nous ne répondrons en règle générale plus aux demandes des départements et des offices, à moins qu'elles ne proviennent du conseiller à la protection des données de l'office ou du département. Il reviendra ainsi à l'avenir au conseiller à la protection des données dans les départements et dans les offices d'assumer les tâches d'accompagnement de projets et de conseil. Les organes qui traitent des données personnelles et qui mettent en place des projets d'informatisation sont en effet les premiers responsables d'assurer le respect des dispositions fédérales de protection des données. Ils doivent se procurer les connaissances nécessaires en la matière. Nous continuerons à soutenir, dans la mesure de nos capacités, les organes fédéraux et en première ligne les conseillers à la protection des données. Toutefois tout comme dans le secteur privé, notre activité de conseil se concentrera sur les cas qui nécessitent des connaissances particulières ou qui revêtent une sensibilité spécifique. Cela n'exclut par contre pas que nous prenions position, le moment opportun, sur un projet spécifique dans le cadre de nos tâches de surveillance.

12.2 La dixième Conférence suisse des Commissaires à la protection des données

La dixième Conférence suisse des Commissaires à la protection des données a eu lieu le 20 novembre 2003 à Genève. Le thème majeur choisi cette année était la publicité électronique non sollicitée (spam).

La publicité électronique non sollicitée (spam) est un problème mondial qui se pose surtout aux entreprises car ces messages publicitaires nécessitent de grosses capacités de mémoire et génère des coûts en conséquence. Les spams inondent aussi les boîtes à lettres électroniques des particuliers d'informations que ceux-ci n'ont pas demandées, sans oublier les adresses électroniques privées qui non seulement servent à faire parvenir des messages non souhaités, mais aussi, dans bien des cas, sont transmises à des tiers sans le consentement de la personne concernée.

Cette conférence a été l'occasion de traiter et de discuter des divers aspects juridiques et techniques de ce problème. Celui-ci ne peut être résolu uniquement sur la base de dispositions légales internes. Au contraire, il convient de mettre en place des réglementations internationales pour que d'une part les expéditeurs des spams puissent être identifiés et d'autre part, pour que les plaintes déposées puissent déployer leurs effets au-delà des frontières.

Enfin, les divers aspects techniques des spams ont été analysés et les moyens pratiques de se protéger ont été signalés. Il a été mentionné à cet égard qu'indépendamment des dispositions légales dont l'efficacité est actuellement limitée, les utilisateurs des messageries électroniques devraient eux aussi exploiter les possibilités techniques existant actuellement pour se défendre contre les spams.

12.3 Les publications du PFPD – Nouvelles parutions

- Aide-mémoire concernant les expertise demandées par les assureurs en responsabilité civile
- Explications sur la vidéosurveillance sur le lieu de travail
- Explications sur la surveillance téléphonique sur le lieu de travail
- Explications sur les prises de références lors d'une candidature
- Remaniement du guide sur la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail

Le guide publié en 2001 sur la surveillance de l'utilisation d'Internet et du courrier électronique sur le lieu de travail a fait l'objet d'une révision approfondie. Les travaux de remaniement portent à la fois sur les aspects techniques et sur le déroulement de la surveillance. Un nouveau règlement-type sur la surveillance ainsi que de nouveaux schémas complètent le nouveau guide que l'on peut consulter sur le site Internet du PFPD (http://www.edsb.ch/f/doku/leitfaeden/internet/index.htm).

Site Internet du PFPD

Sur notre site Internet, sous la rubrique «Qui est le préposé», nous avons créé une nouvelle rubrique «Contact» dont le but est d'aider les citoyens dans leur recherche d'informations au sujet de la protection des données. Quiconque a des questions sur la protection des données trouvera sur cette page, groupés par thèmes, une liste de liens vers des informations disponibles sur notre site Internet. Si une question n'y trouve malgré tout pas sa réponse, il existe la possibilité de nous faire parvenir une brève demande à l'aide d'un formulaire de contact (pour les demandes plus longues, nous vous prions de nous les soumettre sous forme de lettre). La demande est transmise sous forme cryptée du poste de travail de l'expéditeur au serveur de l'administration fédérale et depuis là sous forme non cryptée au PFPD. Si vous voulez que votre message soit transmis de manière cryptée depuis votre station de travail jusqu'au PFPD, veuillez envoyer un message crypté à l'aide de PGP. Vous trouverez de plus amples informations sur le formulaire de contact sous:

https://sec3.admin.ch/edsb/f/service/kontaktF.htm

Nouvelles informations dans différents domaines:

- Explications sur l'exploitation de caméras web conforme aux exigences de la protection des données

  (http://www.edsb.ch/f/themen/video/webcam.f.pdf)

- Explications sur les prises de références lors d'une candidature

  (http://www.edsb.ch/f/themen/weitere/referenzauskuenfte_f.pdf)

- Explications sur les applications actuelles de la stéganographie

  (http://www.edsb.ch/f/themen/sicherheit/technik/steganographie_f.pdf)

- Questions et réponses concernant le domaine des assurances

  (http://www.edsb.ch/f/fragen/versicherungen/index.htm)

- Questions et réponses concernant le domaine du commerce et de l'économie

  (http://www.edsb.ch/f/fragen/handel/index.htm)

- Aide-mémoire concernant les expertises demandées par les assureurs en responsabilité civile

  (http://www.edsb.ch/f/doku/merkblaetter/haftpflicht.htm)

- Expertise relative à un identificateur de personnes sous l'angle de la protection de la personnalité prévue dans le droit constitutionnel

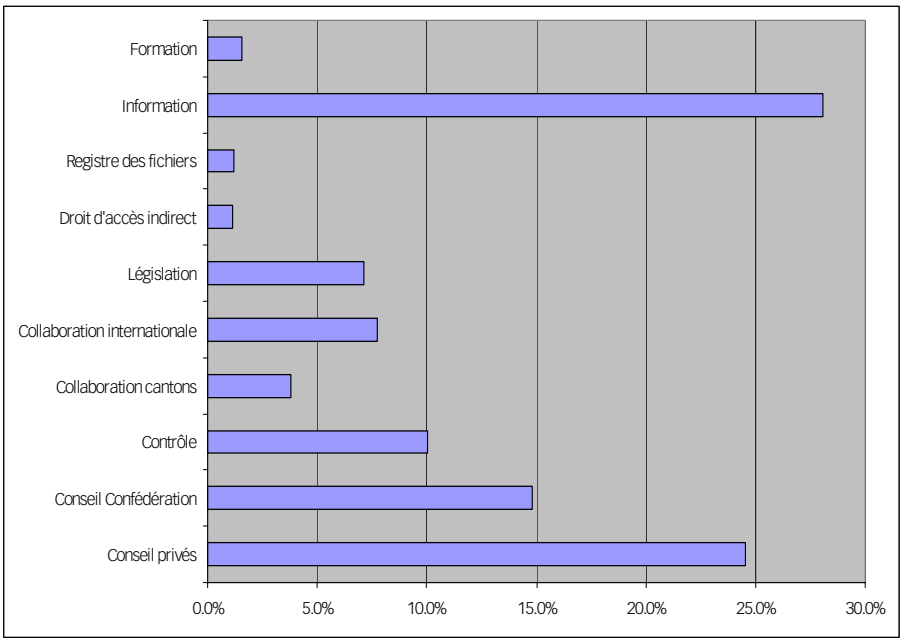
  (http://www.edsb.ch/f/themen/weitere/epid/epid.htm)

- Document de base du PFPD sur les possibilités, limites et conditions d'un identificateur fédéral de personnes harmonisé sous l'angle de la protection de la personnalité

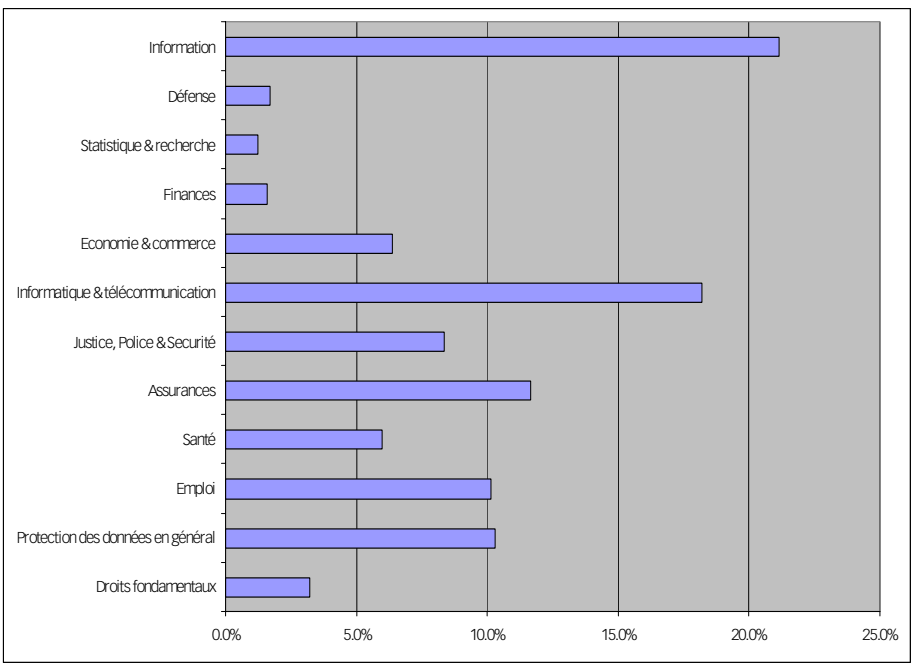
  (http://www.edsb.ch/f/themen/weitere/epid/epid.htm)

12.4 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2003 au 31 mars 2004

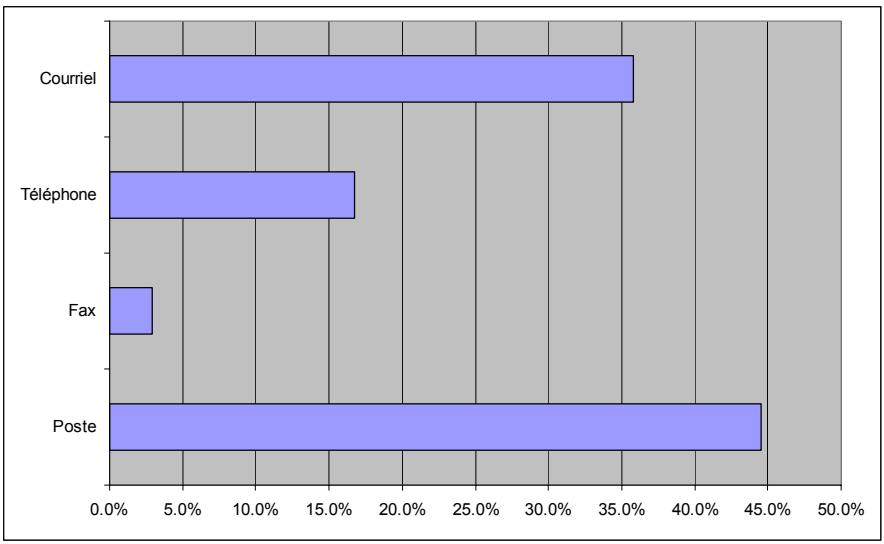
Charge de travail par tâches



Charge de travail par domaine



Provenance des demandes



12.5 Secrétariat du Préposé fédéral à la protection des donnés

Préposé féderal à la protection des données:	Thür Hanspeter, Fürsprecher
Suppléant:	Walter Jean-Philippe, Dr. iur.
Secrétariat:	
Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité Conseil et Information:	8 personnes
Unité Surveillance:	9 personnes
Chancellerie:	3 personnes

13. Annexes

13.1 Explications sur la vidéosurveillance sur le lieu de travail

1. Problématique

L'expérience montre que les équipements de vidéosurveillance, très répandus de nos jours notamment sous la forme de webcams, éveillent un malaise chez les travailleurs concernés et altèrent l'ambiance générale au travail. Ces appareils peuvent porter atteinte au bien-être, à la santé psychique et, par conséquent, à l'aptitude au travail du personnel. Il est donc dans l'intérêt de tous les acteurs de n'utiliser les appareils de vidéosurveillance que si des mesures moins radicales ne permettent pas d'atteindre le but recherché.

2. Bases juridiques

L'employeur est tenu de protéger et de respecter la santé et la personnalité du travailleur[1]. En ce qui concerne la surveillance, cela signifie que les caméras vidéo visant à contrôler le comportement des personnes ne sont pas autorisées. Si elles sont nécessaires pour d'autres raisons, elles doivent être conçues et utilisées de sorte à ne pas porter atteinte à la santé ou à la liberté de mouvement du travailleur[2]. Par ailleurs, 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 (LPD, RS 235.1) sont applicables[3]. Il faut garder à l'esprit notamment l'art. 13 LPD, selon lequel une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public ou par la loi.

3. Conditions préliminaires

Les conditions qui valent ici sont les mêmes que celles énoncées dans l'aide-mémoire sur la vidéosurveillance effectuée par des personnes privées. S'y ajoute le fait que les travailleurs ou leurs représentants ont un droit de regard avant la mise en service d'un système de vidéosurveillance.

[1] Art. 328 du code des obligations (CO, RS 220).
[2] Art. 26 de l'ordonnance 3 relative à la loi sur le travail (RS 822.113).
[3] Art. 328b CO.

Il est également conseillé d'utiliser des technologies permettant de protéger les données, par ex. des *filtres* qui brouillent les visages filmés en temps réel (techniques de floutage) et garantissent donc la sphère privée. Si les prises servent à des fins d'identification (p. ex. dans le cadre de poursuites pénales), les images filmées peuvent alors être décryptées par les personnes autorisées.

4. Finalité

- La vidéosurveillance pour des motifs d'organisation, de sécurité ou de contrôle de la production est autorisée. Dans ce contexte, le travailleur ne doit pas être filmé, sauf exception; en effet, dans le cas contraire, sa santé et sa liberté de mouvement en seraient affectées. On peut également envisager d'installer des caméras vidéo pour surveiller les alentours de bâtiments, les parkings, les accès d'immeubles, les couloirs, les machines et les installations dangereuses, les chambres fortes, les installations gazières situées à l'extérieur, les entrepôts contenant des produits dangereux ou de valeur, les guichets des banques, etc.
- Il est concevable de procéder à des enregistrements ponctuels des employés à des fins pédagogiques. Dans ce cas, le fait que les employés connaissent simplement la période choisie pour la prise de vues n'est pas incompatible avec la protection de la personnalité. Selon le principe de la proportionnalité, et en raison des devoirs de protection de la personnalité et de la santé sur le lieu de travail, cette période doit être aussi courte que possible. Ainsi, une période de trois jours apparaît comme suffisante.
- Les systèmes vidéo ayant pour but une surveillance ciblée du comportement d'un travailleur sont interdits. En effet, il n'est pas permis à l'employeur de surveiller le comportement de ses employés, car plusieurs aspects de la personnalité du travailleur en seraient affectés. Cela toucherait notamment à la sphère privée, voire à l'intimité ou aux relations familiales d'un ou de plusieurs travailleurs. Une telle surveillance pourrait en outre nuire à la santé d'un travailleur si elle était permanente, car ce dernier se sentirait constamment sous pression. Enfin, surveiller le comportement sans prévenir les intéressés serait contraire au principe de la bonne foi[4].

[4] Art. 4, al. 2, LPD.

5. Surveillance vidéo en cas d'infraction pénale ou de présomption d'infraction pénale

S'il y a infraction pénale ou présomption d'infraction pénale, il est possible de mettre un travailleur sous surveillance, à condition que cette mesure ait été ordonnée par voie judiciaire suite à une dénonciation contre inconnu. Pour l'exécution du droit à l'information dans le cadre d'une procédure en cours, ce ne sont pas les dispositions de la loi sur la protection des données qui s'appliquent, mais les règles correspondant à la procédure en question[5].

A titre exceptionnel, l'état de nécessité[6] peut justifier l'utilisation d'un système de surveillance par l'employeur. De même, l'utilisation d'une caméra vidéo est possible en cas de présomption d'une infraction pénale et à condition d'informer les employés au préalable sur une surveillance limitée dans le temps.

6. Prétentions du travailleur en cas de surveillance illicite

Si la surveillance n'est pas justifiée par la nécessité, les enregistrements de l'employeur montrant le comportement d'un travailleur risquent d'être considérés comme des preuves non recevables. Ils peuvent en outre avoir des conséquences tant civiles[7] que pénales[8].

7. Exemples

7.1 Exemple 1: vidéosurveillance sur des chantiers

De nos jours, il est fréquent de trouver des équipements de vidéosurveillance sur les chantiers. Le but invoqué est de faire face aux risques de vol, mais aussi d'économiser des frais en permettant de contrôler l'avancement des travaux à distance. Or, le but de la surveillance vidéo est rarement communiqué aux travailleurs.

La surveillance nocturne par caméra vidéo est en principe justifiée. Les équipements de surveillance sont alors installés pour des raisons de sécurité (prévention des vols) et ne concernent pas le personnel.

[5] Art. 2, al. 2, let. c, LPD.
[6] Art. 34 du code pénal (CP).
[7] Art. 15 ou 25 LPD.
[8] Art. 179quater CP.

Par contre, la surveillance diurne pose problème. En principe, il faut éviter d'activer les caméras vidéo pour contrôler la progression des travaux, car ce serait une mesure disproportionnée (principe de proportionnalité énoncé à l'art. 4, al. 2, LPD). L'absence de proportionnalité est également flagrante dans le rapport entre le nombre de personnes ayant un intérêt à la surveillance et le nombre de personnes surveillées. Un système vidéo peut aussi être ressenti comme une façon de surveiller le comportement lorsque les travailleurs concernés ne savent pas exactement dans quel but ce système est mis en place. De plus, même correctement informés, ils peuvent se sentir constamment observés et ce, d'autant plus que les caméras vidéo disposent souvent d'un zoom, ce qui permet d'identifier les personnes et donc de surveiller le comportement.

La surveillance sur les chantiers n'est admise que si toutes les conditions énoncées ci-dessous sont remplies:

- difficulté d'effectuer quotidiennement les constats de visu et nécessité des prises de vues (p. ex. si l'architecte et le maître de l'ouvrage doivent parcourir une grande distance pour contrôler l'avancement des travaux);
- remplacement des caméras vidéo par un appareil photo numérique sans zoom servant à prendre quotidiennement quelques vues de l'avancement des travaux. On évite ainsi le risque d'une surveillance constante du comportement. L'utilisation d'une caméra vidéo n'est possible que si la caméra est orientable, c'est-à-dire qu'elle n'est dirigée vers le chantier que le temps nécessaire à des prises de vues et, le reste du temps, vers un point qui ne peut affecter ni les travailleurs, ni des tiers;
- réalisation des prises de vues, autant que possible, pendant les pauses ou après la journée de travail;
- emploi de technologies permettant de protéger les données (cf. § 3);
- information détaillée aux travailleurs concernés, par écrit, sur le but, les motifs, la nécessité et la fréquence journalière (p. ex. 2 fois par jour) des prises de vues (économies, baisse des frais de coordination, rapport sur l'avancement des travaux). La surveillance du comportement doit être expressément exclue;
- protection des prises de vues par des mots de passe, si celles-ci doivent transiter par l'Internet, et restriction de l'accès à un petit nombre de personnes autorisées, pour une durée déterminée d'avance et limitée (p. ex. pendant les travaux).

7.2 Exemple 2: vidéosurveillance d'employés de kiosques

La vidéosurveillance d'employés de kiosques est interdite, car elle porte atteinte à la sphère privée des employés, voire à leur intimité ou à leurs relations familiales, d'autant plus que la surveillance n'est généralement pas annoncée. Dans la mesure où les employés sont au courant d'une surveillance, leur santé peut également s'en ressentir à cause de la pression constante, offensante, qu'une caméra peut exercer. Or, l'atteinte au domaine privé par l'intermédiaire d'appareils enregistreurs relève du droit pénal. Il est concevable de surveiller un employé de kiosque en cas d'infraction pénale ou de présomption d'infraction pénale (surveillance contre le vol) si cette mesure est ordonnée par une instance judiciaire. Exceptionnellement, on pourrait envisager la vidéosurveillance par l'employeur si elle est dictée par la nécessité. Mais, dans ce cas, l'employeur serait tenu de demander l'autorisation aux autorités compétentes dans les meilleurs délais pour pouvoir éventuellement poursuivre la surveillance. Il est aussi envisageable d'utiliser une caméra vidéo qui ne se déclencherait que lors de l'ouverture de la caisse et qui se désactiverait automatiquement, dès la fermeture de la caisse, d'une manière identifiable par l'employé. En toute état de cause, il convient d'utiliser un filtre pour le floutage de l'image (cf. § 3).

Les règles relatives à la surveillance de tiers par la vidéo du kiosque demeurent réservées.

7.3 Exemple 3: vidéosurveillance dans les grands magasins et les banques

Les magasins sont souvent équipés d'installations de surveillance. Ces dernières ne doivent pas être utilisées pour surveiller les employés. Pourtant, les employés sont souvent les premiers concernés. Les caméras vidéo doivent donc être orientées et cadrées de sorte que le personnel de vente ne soit pas constamment filmé. L'orientation et les réglages des caméras vidéo doivent donc faire l'objet d'une discussion avec les employés afin que ces derniers connaissent les zones non filmées. Dans ce cas aussi, il convient de recourir au floutage (cf. § 3).

Les caméras vidéo des salles de guichets de banques, utilisées pour des raisons de sécurité, doivent être positionnées de façon à ce que le personnel de la banque ne soit dans le champ de la caméra qu'exceptionnellement.

7.4 Exemple 4: vidéosurveillance dans un centre de tri postal

Le cas de la surveillance dans un centre de tri postal a été traité dans le 7e Rapport d'activités 1999/2000 du Préposé fédéral à la protection des données, disponible sous:

http://www.edsb.ch/f/doku/jahresberichte/tb7/kap7.htm.

7.5 Exemple 5: vidéosurveillance dans un atelier d'orfèvre

A condition que l'atelier ne soit pas l'objet d'une surveillance constante, l'employeur est autorisé à défendre ses propres intérêts en utilisant des caméras de vidéosurveillance aux points stratégiques de l'entreprise: entrées, fenêtres, vestiaire. La surveillance du vestiaire d'un atelier d'orfèvre peut être une mesure appropriée pour découvrir des vols commis par des employés, mais ce n'est pas nécessairement la meilleure solution. Un détecteur de métaux serait plus efficace, pour autant qu'il soit proportionné sur le plan des coûts. Les détecteurs de métaux peuvent reconnaître différentes sortes de métaux et émettre un signal différencié selon le métal détecté. Dans cet exemple, les employés peuvent se changer au vestiaire pour revêtir une tenue de travail contenant aussi peu de métal que possible. En quittant le lieu de travail, ils seraient soumis au détecteur de métaux avant de pouvoir récupérer leurs effets personnels, pour lesquels il importe peu qu'ils contiennent du métal ou non. Les lunettes, les montres et autres objets métalliques indispensables aux employés pendant le travail doivent être mis de côté.

13.2 Explications sur la surveillance téléphonique sur le lieu de travail

1. Introduction

Le téléphone fait partie des moyens de communication les plus courants sur le lieu de travail. Il est utilisé pour des raisons professionnelles aussi bien que personnelles. En ce qui concerne la surveillance téléphonique, l'employeur est tenu de protéger et de respecter la personnalité du travailleur[1], en particulier sa sphère privée.

De son côté, le travailleur doit exécuter avec soin le travail qui lui est confié et sauvegarder fidèlement les intérêts légitimes de l'employeur[2]. L'usage de systèmes de surveillance pour contrôler le respect du règlement relatif au téléphone peut représenter une atteinte inadmissible à la sphère privée du travailleur si certaines conditions ne sont pas observées[3]. Le travailleur lésé peut intenter une action civile en cas d'atteinte à sa personnalité; il peut en outre déposer une plainte pénale[4].

[1] Art. 328 du Code des obligations (CO), RS 220.
[2] Art. 321a CO.
[3] Art. 26 de l'ordonnance 3 relative à la loi sur le travail (OLT 3), RS 822.113.
[4] Art. 179bis du Code pénal (CP), RS 311.0.

L'employeur doit protéger les données relatives aux communications téléphoniques en prenant les mesures nécessaires, en termes de technique et d'organisation, contre une utilisation non autorisée de ces données. Il assure en particulier la confidentialité, la disponibilité et l'exactitude des données[5]. Le travailleur peut à tout moment demander à son employeur si des données le concernant sont traitées et, le cas échéant, lesquelles et dans quel but[6].

2. Conditions justifiant la surveillance

S'il n'existe pas de règlement sur l'utilisation du téléphone, il est impossible de savoir clairement quelles sont les dispositions en la matière. En l'absence de restriction expresse ou d'interdiction des appels privés sur le lieu de travail, le travailleur peut considérer que l'usage privé du téléphone est autorisé, dans les limites du raisonnable, et qu'aucune surveillance n'a été mise en place. En tout état de cause, les intérêts et les moyens de l'employeur doivent être préservés.

Si l'employeur souhaite surveiller les communications téléphoniques sur le lieu de travail, il doit observer les conditions suivantes:

2.1 Information préalable

2.1.1 Règlement concernant l'utilisation du téléphone

La question de savoir si le travailleur a le droit d'utiliser le téléphone à des fins privées dépend avant tout de la volonté de l'employeur (droit d'édicter des directives et des instructions, art. 321d CO, RS 220). A noter que même si les appels privés sont interdits, cela n'inclut pas la réception des communications privées sur son lieu de travail.

Publier une directive sur l'utilisation du téléphone est une bonne chose, même si ce n'est pas obligatoire, car ce type de règlement écrit assure la transparence et la sécurité juridique dans les relations entre l'employeur et le travailleur. En effet, un règlement communiqué oralement est tout aussi contraignant, mais, en cas de litige, il est difficile de fournir des preuves.

Selon le règlement d'utilisation, les communications privées peuvent être autorisées, limitées ou interdites. Pour limiter l'usage du téléphone, différents moyens sont possibles: on peut ainsi empêcher techniquement les appels internationaux ou bloquer certains numéros de téléphone, ou encore fixer des horaires pendant lesquels les appels privés sont autorisés. Un grand nombre d'entreprises prennent à leur compte le coût des appels privés de leurs employés jusqu'à un montant déterminé d'avance.

[5] Art. 8, al. 1, de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD), RS 235.11.
[6] Art. 8 LPD, RS 235.1.

2.1.2 Information sur la surveillance

Si le règlement n'est pas obligatoire, l'employeur a en revanche le devoir d'informer les travailleurs d'une éventuelle surveillance dont leurs communications téléphoniques feraient l'objet, car celle-ci peut représenter une atteinte à la sphère privée des travailleurs (principe de la bonne foi, art. 4, al. 2, LPD). Cette information préalable concerne notamment le système de surveillance utilisé et le mode opératoire. Il faut que les travailleurs aient été préalablement informés de la possibilité de ces contrôles et de l'éventualité de sanctions si les contrôles signalent une utilisation abusive du téléphone. Il faut les informer également, le cas échéant, qu'un système d'écoute des conversations est mis en place à des fins de contrôle de la performance ou de preuve et leur expliquer les conditions associées à ces contrôles. Il est également conseillé de préciser aux personnes concernées qui est responsable de la journalisation différenciée des appels ou de l'écoute des conversations, quelles sanctions concrètes peuvent être prises sur le plan du droit du travail et de quelle manière une action pénale peut être intentée en cas de soupçon. Enfin, il convient d'exposer les mécanismes permettant de différencier les appels privés des appels professionnels. Les droits d'accès, le contenu et la durée de conservation des données journalisées font aussi partie des informations à communiquer.

C'est pourquoi il est conseillé d'édicter un règlement sur la surveillance du téléphone, rédigé par écrit pour des raisons de transparence et de sécurité juridique, et qui sera joint au règlement concernant l'utilisation du téléphone en un même document.

2.2 Comment différencier les appels privés des appels professionnels

Pour que la sphère privée du travailleur soit protégée, il faut pouvoir distinguer les appels selon leur nature. Ainsi, lors de l'évaluation des données concernant des appels privés, seul l'indicatif des numéros composés à titre privé devrait être consigné, et la teneur des conversations privées ne doit pas faire l'objet d'une surveillance.

S'il s'agit d'appels sur le réseau de téléphonie fixe, avec les moyens techniques appropriés, par exemple un central téléphonique dans l'entreprise, le travailleur peut différencier les appels privés des appels professionnels en appuyant sur une touche avant la communication.

En l'absence de tels moyens, ou si les bureaux ne permettent pas de mener des conversations privées, il convient de prévoir un appareil mis à la disposition de l'entreprise, non surveillé et financé par les travailleurs (p. ex. cabine téléphonique) ou de permettre l'utilisation d'un téléphone privé (p. ex. un téléphone mobile).

La différenciation des appels par une touche ou la mise à disposition d'une cabine téléphonique par l'employeur présentent un inconvénient dans la mesure où l'entre-

prise est partenaire contractuelle du fournisseur de services de télécommunication: sur la facture, les données complètes des appels sortants apparaissent, aussi bien pour les appels privés que pour les professionnels.

La loi sur les télécommunications autorise l'employeur à demander au fournisseur de services de télécommunication des paramètres d'adressage identifiables dans sa facturation. Il est recommandé de régler ce problème avec le fournisseur, d'en parler avec le travailleur et de le mentionner dans les directives internes concernant l'utilisation du téléphone sur le lieu de travail. L'employeur doit explicitement demander au fournisseur de restreindre à l'indicatif le relevé des numéros signalés comme privés.

La différenciation entre les appels entrants privés et professionnels est plus problématique. Elle pourrait être envisagée pour contrôler la teneur des conversations, mais cela n'est juridiquement admissible qu'aux conditions énoncées au point 3.2. Une différenciation partielle des données techniques des appels entrants serait également possible si ces derniers étaient journalisés et comparés avec une liste de numéros privés. Ce type de contrôle peut se justifier par des intérêts tels que la nécessité de ne pas occuper la ligne, mais ne doit pas avoir pour objectif d'empêcher que le travailleur soit joignable.

En ce qui concerne le réseau de téléphonie mobile, la manière la plus simple de différencier les appels sortants professionnels des appels privés est d'utiliser deux cartes SIM.

3. Objet et but de la surveillance

3.1 Surveillance des données techniques

La surveillance des données techniques par l'employeur sert essentiellement à vérifier si le règlement interne est observé, mais aussi à établir les factures au collaborateur ou au client.

La surveillance des données techniques liées à l'utilisation du téléphone peut être effectuée sur une base régulière. Elle porte sur les données suivantes:

- numéro complet de la personne qui appelle;
- numéros d'appels sortants de nature privée, réduits à l'indicatif;
- numéros complets d'appels sortants de nature professionnelle;
- date et heure des connexions;
- durée;
- coût des communications;

- indications sur la nature de la connexion (réseau fixe ou mobile);
- indications sur la région de tarification: communication nationale ou internationale (+ pays).

Si on constate un abus, le travailleur concerné doit avoir la possibilité de s'en expliquer.

On ne peut consigner des numéros complets d'appels privés qu'à des fins de preuve, soit parce que le collaborateur en a exprimé le souhait, soit parce que c'est nécessaire dans le cadre d'un litige.

Les données techniques concernant les communications téléphoniques ne doivent pas être conservées plus de six mois.

3.2 Ecoute des conversations

3.2.1 Conversations privées

L'employeur n'est pas autorisé à écouter ni à enregistrer les conversations privées, parce qu'une telle surveillance n'est pas nécessaire à l'exécution du contrat de travail[7], qu'elle constitue une atteinte à la personnalité du travailleur[8] et qu'elle peut faire l'objet de poursuites pénales[9]. S'il est nécessaire de réunir des preuves dans le cadre d'une poursuite pénale, il faut que ce soit sur ordre des autorités compétentes. Sont réservées les dispositions relatives à l'état de nécessité[10]. Dans ce cas, l'employeur est tenu de passer le relai aux autorités compétentes pour la poursuite de la surveillance.

3.2.2 Conversations professionnelles

a. Buts

L'écoute ou l'enregistrement des conversations par l'employeur sont admis dans les buts suivants:

- obtention de preuves;
- contrôle de performance.

[7] Art. 328b CO.
[8] Art. 328 CO ; art. 26 OLT 3, RS 822.113.
[9] Art. 179bis Code pénal (CP), RS 311.0.
[10] Art. 34 CP.

b. Conditions

Le Code pénal pose comme condition préalable à l'écoute ou à l'enregistrement des conversations le consentement de tous les participants[11]. Les personnes dont la conversation est enregistrée ou mise sur écoute doivent en être informées sans ambiguïté et en temps utile; en outre, elles doivent donner leur accord. Informer les personnes concernées au préalable permet également d'éviter l'écoute ou l'enregistrement de conversations privées. Il n'est pas indispensable de redonner cette information à chaque conversation téléphonique si l'écoute ou l'enregistrement sont systématiques et que les interlocuteurs en ont déjà été informés sans équivoque. Cette solution est envisageable dans certains secteurs bancaires, par exemple, où des affaires juridiques doivent être traitées par téléphone. Il suffit alors de mentionner de manière explicite l'existence d'un système d'écoute ou d'enregistrement, dans le contrat de travail pour les employés et dans les conditions générales pour la clientèle. On peut également informer les employés dans le contrat de travail et prévoir un message préenregistré pour informer l'ensemble des interlocuteurs qui ne sont pas sous contrat. Il se peut aussi que les conversations téléphoniques aient pour participants des clients informés par contrat et des personnes non liées contractuellement à l'entreprise. Dans ce cas, les premiers sont informés dans les conditions générales, mais les seconds doivent à chaque fois être informés oralement de l'écoute ou de l'enregistrement des conversations.

L'écoute ou l'enregistrement occasionnels de conversations de tiers sont envisageables dans le cadre d'un centre d'appels. En règle générale, les employés sont informés chaque fois que leur conversation est mise sur écoute, au moyen d'un signal optique ou acoustique. Dans la perspective d'une meilleure observation des intérêts de l'employeur, notamment pour le contrôle de la qualité et l'efficacité de la formation, informer les employés de l'écoute ou de l'enregistrement seulement sur une période déterminée n'est pas incompatible avec la protection de la personnalité. Le principe de la proportionnalité et la protection de la personnalité et de la santé sur le lieu de travail exigent que cette période soit limitée à cinq jours. Bien entendu, le devoir d'informer les autres interlocuteurs est toujours valable (par exemple sous la forme d'un préenregistrement qui se déclenche au début de la conversation).

L'employeur peut conserver les enregistrements jusqu'à ce que le but recherché soit atteint et doit ensuite les détruire.

[11] Art. 179bis CP.

L'enregistrement d'appels de détresse pour le compte de services d'assistance, de secours ou de sécurité n'est pas punissable[12].

3.3 Surveillance en cas d'infraction

Si l'employeur a de bonnes raisons de soupçonner qu'une infraction a été commise ou va être commise par téléphone, il peut alors s'assurer de la journalisation des données techniques liées à l'usage du téléphone. Ses soupçons peuvent reposer sur un comportement qui, au-delà d'un manquement au contrat de travail ou au règlement concernant l'utilisation du téléphone, remplit les conditions de l'infraction, par exemple une atteinte à la réputation de l'employeur ou un cas de harcèlement sexuel sur le lieu de travail[13]. L'employeur n'a aucune obligation de dénonciation, mais il est recommandé, au moins pour les infractions poursuivies d'office, de les dénoncer pour éviter toute complicité. Ordonner la surveillance de la teneur des conversations pour réunir des preuves ou confirmer un soupçon relève des autorités de poursuite pénale. L'employeur ne doit pas prendre l'initiative de mettre sur écoute ou d'enregistrer une conversation téléphonique (cf. chapitre 3.2.a). Du reste, un tel procédé serait considéré comme une preuve non valable dans une procédure judiciaire. Les autorités compétentes de poursuite pénale ordonnent une surveillance si, dans le cadre de la pesée des intérêts en présence, un intérêt prépondérant privé ou public est établi. L'employeur doit traiter les informations obtenues par la surveillance de manière confidentielle à l'égard des tiers, en particulier de ses autres travailleurs. Sont réservées les sanctions prévues en droit du travail par une atteinte au règlement concernant l'utilisation du téléphone.

4. Sanctions en cas d'abus

Tout en observant les conditions et les règles de la surveillance, s'il constate un abus de l'utilisation du téléphone, l'employeur peut prononcer contre le travailleur fautif des sanctions relevant du droit du travail. Le travailleur répond du dommage qu'il cause à l'employeur intentionnellement ou par négligence[14].

[12] Art. 179quinquies CP. N'est pas non plus punissable l'enregistrement sans avertissement préalable de conversations téléphoniques dans les relationsd'affaires, lorsqu'il a une valeur de preuve.
[13] Art. 198 CP.
[14] Art. 321e CO.

La sanction peut se présenter sous forme d'un blâme ou d'une action en dommages-intérêts. Dans des cas extrêmes, lors d'abus répétés en dépit d'un blâme ou lors d'une infraction avérée, l'employeur peut même résilier le contrat[15]. L'employeur ne peut résilier immédiatement le contrat que si les circonstances ne permettent pas, selon les règles de la bonne foi, d'exiger de lui la continuation des rapports de travail[16].

Les sanctions doivent être prononcées par le supérieur du travailleur fautif. Elles doivent être proportionnelles à l'abus et leur étendue doit être définie dans le règlement concernant la surveillance ou pouvoir être déduite de ce règlement.

En ce qui concerne la charge de la preuve, la règle qui prévaut est la suivante: l'employeur doit prouver que le travailleur a failli à ses obligations et qu'il en résulte un dommage. Ensuite, c'est au travailleur de prouver qu'aucune faute ne lui est imputable ou que sa faute est légère[17].

5. Prétentions du travailleur en cas de surveillance non admissible

Si l'employeur ne respecte pas les règles et les conditions relatives à la surveillance téléphonique, il peut être attaqué en justice pour atteinte illicite à la personnalité (art. 15 et 25 LPD). La charge de la preuve est réglementée par l'art. 97 CO. Le travailleur concerné peut commencer par faire valoir ses prétentions (établissement du caractère illicite, dommages-intérêts, etc.) auprès de son employeur. Si ce dernier ne répond pas aux prétentions du travailleur, le juge du travail peut être sollicité. En règle générale, cette procédure est rapide et gratuite. Même les sanctions en application du droit du travail prononcées du fait d'un abus constaté à la suite d'une surveillance peuvent être dénoncées (p. ex. congé abusif, art. 336 CO).

En cas de surveillance abusive, l'employeur peut aussi s'exposer à des actions pénales, par exemple en cas d'écoute ou d'enregistrement d'une conversation entre d'autres personnes[18].

[15] Art. 335 CO.
[16] Art. 337 CO.
[17] Art. 97 CO.
[18] Art. 179bis CP.

6. Caractéristiques particulières des installations téléphoniques

Les caractéristiques techniques des installations téléphoniques modernes à transmission numérique (en particulier les raccordements de type ISDN-RNIS) offrent de nombreux avantages pour les utilisateurs, mais également des risques de violation de la protection des données. Les paragraphes qui suivent mettent en évidence ces risques et les moyens de les éviter.

6.1 Appareils «mains libres» munis d'un haut-parleur

Les appareils munis d'un haut-parleur et d'un microphone peuvent être utilisés sans que le destinataire de l'appel soulève le combiné. L'appelant peut être entendu dans le local où se trouve le destinataire et suivre le cas échéant les conversations qui ont lieu dans ce local.

Problème:

Les conversations des personnes situées au voisinage immédiat de l'appareil de téléphone peuvent être entendues à l'insu de ces personnes par l'interlocuteur, tandis que les propos de celui-ci peuvent être entendus par les personnes susmentionnées.

- L'interlocuteur dont la voix est commutée sur haut-parleur doit être informé que ses propos peuvent être suivis par d'autres personnes présentes dans la pièce.
- Les personnes qui se trouvent dans un local où un entretien téléphonique se déroule au moyen d'un dispositif «mains libres» doivent être informées que leurs propos peuvent être entendus par des tiers.

6.2 Affichage du numéro de l'appelant

Avant même la réception d'un appel téléphonique, le numéro de l'appelant s'affiche (le cas échéant aussi ses nom et prénom).

Problème:

En cas d'affichage systématique du numéro de l'appelant, celui-ci ne peut garder son identité secrète ni l'endroit d'ou il appelle (le problème se pose par exemple lorsqu'une personne s'adresse à une unité de conseil interne). L'affichage peut en outre être lu par des tiers, qui prennent ainsi connaissance de l'identité de l'appelant.

- L'appelant doit disposer de la possibilité de supprimer l'affichage de son numéro quand il le souhaite.

6.3 Liste des appelants

Le numéro et l'heure de chaque appel sont enregistrés dans la liste des appelants (que l'on ait répondu ou non à l'appel). De cette manière, l'appelé peut, après une absence, constater qui a tenté de l'appeler et décider, le cas échéant, de rappeler la personne.

Problème:

Il est possible de constater, à l'insu de l'appelant, qu'il a tenté d'appeler à un moment déterminé. Dans certaines circonstances, la liste des appelants peut parvenir à la connaissance de tiers.

- La possibilité de supprimer l'affichage dans certains cas permet d'éviter des entrées non désirées dans la liste des appelants.
- Les listes d'appelants doivent être protégées contre tout accès illicite.

6.4 Annonce directe ou par haut-parleur

Ce système permet de s'adresser à un collaborateur par le haut-parleur du téléphone sans qu'il ait à soulever le combiné ou à actionner une quelconque fonction.

Problème:

 Outre le fait que ce procédé dérange les collègues, il permet également d'écouter des personnes qui ne se sont pas aperçues que l'appareil est enclenché.

- L'annonce par haut-parleur devrait être limitée à certains buts spécifiques.
- La possibilité de procéder à une annonce par haut-parleur doit être clairement signalée.
- L'appareil doit être muni d'un dispositif permettant d'empêcher les annonces non désirées.

6.5 Conférence téléphonique

Un dispositif de conférence (modulable) permet de faire participer d'autres interlocuteurs à une discussion.

Problème:

Il est possible de permettre à des tiers de suivre la conversation à l'insu des autres interlocuteurs.

- Chaque fois qu'un interlocuteur est connecté ou déconnecté, cela doit être signalé (de manière différenciée) à tous les participants.

- Il est souhaitable que chaque interlocuteur puisse déterminer le nombre de participants et leur identité.

6.6 Touches programmables / voyants

Certains appareils téléphoniques sont munis de touches programmables pourvues d'un voyant. L'activation de la touche revient à sélectionner le destinataire. Le voyant indique si l'abonné est au téléphone et, le cas échéant, s'il s'agit d'une liaison interne ou externe.

Problème:

Ce dispositif permet d'observer l'usage du téléphone par les collaborateurs. Lorsque deux voyants s'allument et s'éteignent en même temps, il est même possible de tirer avec une forte probabilité des conclusions sur les communications internes établies entre les collaborateurs et leurs interlocuteurs.

- Ce dispositif ne doit pas aboutir à un contrôle à l'insu des interlocuteurs.
- Les touches ne doivent pas pouvoir être programmées librement de manière à activer des fonctions non prévues.

13.3 Explications sur les prises de références lors d'une candidature

1. Problématique:

Dans le domaine de la prise de références, la théorie et la pratique semblent diverger. Un point particulièrement controversé est celui de savoir si les références ne peuvent être communiquées qu'avec l'assentiment du candidat. L'entrée en vigueur de la loi sur la protection des données a nourri les espoirs de trouver une solution. Mais la situation de droit et la pratique continuent à rester incertaines. Ce document a pour objet de tenter d'éclaircir la question.

2. Définition, finalité et personnes impliquées

Une référence est une information sur le rendement et le comportement d'un employé qui est fournie par l'employeur actuel ou par un ancien employeur à un nouvel employeur potentiel. Le but des ces renseignements est de compléter si nécessaire les informations contenues dans le dossier de candidature et les autres éléments de décision. Une fourniture de références implique en règle générale au moins trois personnes: le candidat, son employeur actuel ou précédent et l'employeur potentiel.

3. Fourniture de renseignements par le candidat

Afin de protéger ses propres biens juridiques ainsi que les biens juridiques des personnes desquelles il répond, le nouvel employeur potentiel a un intérêt à obtenir des informations sur le candidat. C'est pourquoi le nouvel employeur potentiel est autorisé, pour la conclusion du contrat de travail, de traiter les données concernant le candidat dont il a besoin pour déterminer si ce dernier présente les qualités requises pour le poste envisagé. Il n'est cependant pas autorisé à traiter toute autre information dont il n'a pas besoin (principe de la proportionnalité, art. 328b CO). Si le candidat fournit des indications fausses ou cache des informations essentielles, il répond pour le dommage ainsi causé à l'employeur dupé (culpa in contrahendo, art. 97ss CO). Dans les cas par contre où une question inadmissible est posée au candidat, ce dernier ne doit encourir aucun préjudice du fait qu'il ne fournit aucune réponse ou une réponse fausse (droit au mensonge comme légitime défense découlant de son droit d'autodétermination sur les informations personnelles).

4. Prise de références par l'employeur potentiel

Le nouvel employeur potentiel ne peut prendre des renseignements auprès de l'employeur actuel ou précédent qu'après avoir obtenu l'accord du candidat. Il peut cependant admettre un accord tacite si le candidat indique des références dans son dossier de candidature. Si l'accord n'est pas donné, il est illicite de prendre des références car l'employeur actuel ou précédent serait ainsi informé de la candidature. Dans un tel cas, le candidat pourrait faire valoir à l'égard de l'employeur potentiel ses droits pour atteinte à la personnalité (art. 15 LPD).

5. Fourniture de références par l'employeur actuel ou par un ancien employeur

Vu la relation particulière de dépendance économique et personnelle qui existe entre un candidat et son employeur, l'employeur actuel ou précédent a un devoir d'assistance spécial vis-à-vis du candidat (protection de la personnalité, art. 328 CO). L'employeur actuel ou précédent n'est donc pas autorisé à fournir des renseignements sans le consentement du candidat. Ceci vaut également pour les renseignements concernant des aspects essentiels de la relation de travail et découle de l'art. 330a al.2 CO. Ce dernier stipule qu'un employé peut demander à son employeur de lui remettre non pas un certificat de travail, mais une simple attestation d'emploi qui ne mentionne que la nature et la durée des rapports de travail. Cette disposition a été prévue par le législateur pour soumettre la fourniture de renseignements par l'intermédiaire d'un certificat de travail au droit à l'autodétermination en matière d'informations du candidat. Le même raisonnement doit logiquement valoir également pour la

fourniture de renseignements par oral. Car, si l'employeur actuel ou précédent fournissait des renseignements concernant le candidat sans l'accord de ce dernier, cette disposition contraignante (art. 330a al. 2 en liaison avec l'art. 362 CO) serait dépourvue de son sens. C'est la raison pour laquelle l'employeur actuel ou précédent n'est pas tenu de fournir des renseignements s'il na pas l'accord du candidat; s'il le fait néanmoins, il répond des conséquences d'une fausse information à l'égard de l'employeur potentiel et de l'atteinte à la personnalité à l'égard du candidat (art. 165 LPD). D'autre part, le candidat concerné peut porter plainte en vertu de l'art. 35 LPD contre l'employeur actuel ou précédent si celui-ci a intentionnellement communiqué sans autorisation des données personnelles sensibles secrètes ou des profils de la personnalité. Le cas échéant, le candidat peut également intenter une action en justice selon art. 173ss CP.

13.4 Aide-mémoire concernant les expertises demandées par les assureurs en responsabilité civile

I. De quoi s'agit-il ?

En pratique, de nombreux problèmes surgissent entre lésés et assureurs en responsabilité civile au sujet de la protection des données. Concrètement, il s'agit essentiellement de savoir si et à quelles conditions un assureur en responsabilité civile peut demander un avis d'expert à propos d'un lésé. Ces expertises sont demandées à divers spécialistes (médecins, ingénieurs, biomécaniciens, économistes d'entreprise, etc.) et ont pour but d'établir plus clairement une obligation d'indemnisation de l'assureur.

Les conditions dans lesquelles un assureur en responsabilité civile peut demander une expertise sont mal établies. En outre, il faut déterminer si le lésé doit être informé de la demande d'expertise.

II. Considérations juridiques

Les considérations qui suivent se limitent strictement aux aspects liés à la protection des données. Le PFPD ne se prononce pas sur ce qui relève du droit pénal ou d'autres domaines.

Lorsqu'un assureur en responsabilité civile demande une expertise, son acte constitue un traitement de données et doit reposer sur un motif justificatif. En particulier, les assureurs en responsabilité civile ne peuvent, sans motif justificatif, traiter des données personnelles d'un lésé sans le consentement explicite de ce dernier, ni communiquer à des tiers des données personnelles sensibles ou des profils de personnalité.

Un motif justificatif au sens de la loi sur la protection des données ne peut être qu'un consentement de la personne concernée, un intérêt privé ou public prépondérant ou une loi.

Tant le consentement du lésé qu'un intérêt privé ou public prépondérant de l'assureur en responsabilité civile sont des motifs justificatifs primordiaux. Le consentement doit être volontaire et révocable en tout temps.

On ne peut conclure de manière générale à l'existence ou non d'un intérêt privé prépondérant: l'appréciation se fera au cas par cas. Le facteur déterminant est de savoir si l'assureur en responsabilité civile subit un préjudice irréparable en l'absence d'une expertise immédiate. On peut se trouver face à un intérêt privé prépondérant lorsque, par exemple, des raisons médicales empêchent de différer l'expertise. En tout état de cause, le montant du dommage doit être élevé pour que le motif justificatif d'un intérêt privé prépondérant soit recevable (cf. également l'arrêt du Tribunal fédéral 5C.187/1997).

Il convient néanmoins de rappeler qu'il incombe en premier lieu au lésé d'apporter la preuve de la causalité entre le dommage et l'événement (art. 8 CC). On peut dès lors même se demander si, eu égard à la claire attribution du fardeau de la preuve, l'assureur subirait un préjudice s'il laissait le soin au lésé de prouver le dommage, au besoin par une expertise. Le PFPD ne peut toutefois répondre à cette question, qui devra être tranchée un dans cas d'espèce par le juge civil.

Une caractéristique importante du droit de la protection des données est le principe de la transparence. Le traitement, et en particulier la collecte, des données doit être transparent et compréhensible pour la personne concernée. Ce principe s'applique particulièrement aux données personnelles sensibles. Si, par exemple, l'assureur en responsabilité civile veut obtenir une expertise neurologique du lésé, il doit l'en informer.

III. Le PFPD propose d'agir comme suit:

- Par principe, l'assureur en responsabilité civile ne peut obtenir un avis d'expert à propos d'un lésé que sur la base d'un motif justificatif, c'est-à-dire d'un consentement explicite ou d'un intérêt privé ou public prépondérant. Si l'assureur invoque un intérêt privé ou public prépondérant, il doit, dans chaque cas, exposer les motifs justificatifs au lésé.
- L'assureur en responsabilité civile informe le lésé ou son représentant légal de son intention d'obtenir un avis d'expert. Il communique au lésé la portée et le but de l'expertise, en précisant notamment les nom et qualités de l'expert, la teneur du mandat et les documents qui seront transmis à l'expert. L'assureur invite le lésé à donner son avis.

- L'assureur en responsabilité civile donne le mandat à l'expert et y joint les documents nécessaires. Le lésé reçoit une copie du mandat.
- L'assureur en responsabilité civile remet automatiquement une copie du rapport d'expertise final au lésé.

13.5 Résolution relative aux transferts des données des passagers

La 25e Conférence des Commissaires à la protection des données et à la vie privée a adopté la résolution suivante:

A. La Conférence constate que:

1. Dans le cadre de la lutte légitime contre le terrorisme et le crime organisé, des mesures qui sont envisagées dans certains Etats pourraient menacer les droits et les libertés fondamentales et en particulier le droit à la vie privée;
2. En prenant certaines mesures, il y a un danger de porter atteinte à la démocratie et aux libertés au motif de les défendre;
3. Les obligations légales imposant aux compagnies aériennes ou à d'autres transporteurs de fournir un accès à l'ensemble des données relatives aux passagers enregistrées dans les systèmes de réservation ou de les transférer pourraient entrer en conflit avec les principes internationaux de la protection des données ou avec les obligations de ces transporteurs découlant des lois nationales de protection des données.

B. En conséquence, la Conférence affirme que:

1. Dans la lutte contre le terrorisme et le crime organisé, les Etats devraient définir leurs actions en assurant le plein respect des principes fondamentaux de la protection des données, lesquels sont partie intégrante des valeurs défendues;
2. Lorsqu'un transfert international et régulier de données personnelles s'avère nécessaire, il devrait intervenir dans un cadre prenant en compte la protection des données, par exemple sur le fondement d'un accord international fixant les exigences adéquates de protection des données, incluant la définition d'une finalité claire et déterminée, une collecte des données adéquate et non excessive, une durée de conservation des données limitée, l'information des personnes concernées, la garantie des droits des personnes concernées et un contrôle indépendant.

13.6 Document de base du PFPD sur les possibilités, limites et conditions d'un identificateur fédéral de personnes harmonisé sous l'angle de la protection de la personnalité

Voir paragraphe 13.6 de la partie en langue allemande.

13.7 Expertise relative à un identificateur de personnes sous l'angle de la protection de la personnalité prévue dans le droit constitutionnel

Voir paragraphe 13.7 de la partie en langue allemande.

13.8 Décision de la CFPD en matière de droit du bail

no. 16/01

Composition de la Commission

Prof. R. J. Schweizer (Président), Prof. P.-H. Steinauer (juge rapporteur),

Me G. Page; Me M. Sterchi (secrétaire)

DÉCISION

du 28 août 2003

sur la demande du

Préposé fédéral à la protection des données,

Feldeggweg 1, 3003 Berne,

demandeur

dirigée contre

Société X, **Genève**

défenderesse

I. FAITS

a) Suite à la demande d'un particulier, le Préposé fédéral à la protection des données (ci-après: PFPD) a demandé, par lettre du 21 novembre 2000, à la Société X divers renseignements sur les données recueillies auprès des personnes s'intéressant à une location ainsi que la formule d'inscription-type que celles-ci doivent remplir.

b) Le 7 décembre 2000, la Société X a envoyé au PFPD un exemplaire de la formule «Demande de logement» pour les immeubles à loyer contrôlé par l'Etat de Genève ainsi qu'un exemplaire de la formule «Demande de location» utilisée par la Société X pour les immeubles à loyer libre.

c) Le 14 février 2001, le PFPD a demandé à la Société X des informations complémentaires sur le consentement de la personne concernée à la collecte d'informations par une agence de renseignements commer-ciaux. Il a également rendu la Société X attentive au fait que la formule «Demande de location» n'était pas en tous points conforme à la Décision du 21 novembre 1996 de la présente Commission; il se référait aux rubriques «nationalité», «permis de séjour», «salaire annuel», «poursuites» et «loyer mensuel payé actuellement». En ce qui concerne la

«Demande ferme» figurant en page 2 de la formule de la Société X, il renvoyait à la Décision susmentionnée et à ses recommandations du 21 novembre 1994. Enfin, il fixait à la Société X un délai au 31 mars 2001 pour lui communiquer les modifications pro-posées.

d) Le 18 avril 2001, la Société X a envoyé au PFPD une formule modifiée de «Demande de location», avec diverses explications. Cette formule se distinguait notamment de la précédente par une déclaration de consentement de la personne concernée à ce que la Société X prenne «tous renseignements utiles à son sujet en relation avec la présente demande de location».

e) Par lettre du 1er juin 2001, le PFPD a informé la Société X qu'à son avis, la déclaration de consentement proposée n'était pas assez explicite. Il a également constaté que, pour le reste, la Société X n'avait pas donné suite aux suggestions du PFPD et donné diverses justifications de sa position. Il a enfin constaté que la Société X n'avait pas répondu à ses questions sur le recours à une agence de renseignements commerciaux; il a fixé un nouveau délai au 4 juillet 2001 pour ces informations complémentaires.

f) Le 4 juillet 2001, la Société X a donné au PFPD de nouvelles explications sur les motifs pour lesquels elle demande certaines données dans sa formule, en insistant sur le fait qu'il s'agit d'une formule de demande ferme de location. Elle a en outre accepté de se conformer aux suggestions du PFPD relatives aux rubriques «nationalité», «état civil» et «salaire annuel». Elle souhaitait en revanche maintenir telles quelles les autres rubriques, en proposant cependant une déclaration de consentement plus explicite.

g) Le 6 septembre 2001, le PFPD a adressé à la Société X une Recommandation au sens de l'art. 29 al. 3 LPD et portant sur les rubriques «logement actuel», «permis de séjour», «poursuites» et «déclaration de consentement» (à remplacer par une clause facultative d'autorisation) ainsi que sur les documents complémentaires à fournir par le demandeur de logement.

h) Par lettre du 9 octobre 2001, la Société X a communiqué au PFPD qu'elle n'acceptait pas la Recommandation et proposé une nouvelle formule de «Demande de location». Plus précisément, la Société X a accepté de donner un caractère facultatif aux questions sur le numéro de plaques d'immatriculation, le nom et l'adresse du bailleur actuel et le montant du loyer actuel; elle a également accepté de limiter la question sur les poursuites aux deux dernières années. La nouvelle formule du 21 décembre 2001 comporte une rubrique supplémentaire sur les «actes de défaut de biens» et remplace la déclaration de consentement par une question formulée comme suit: «Le soussigné autorise-t-il le bailleur, respectivement la

Société X, à obtenir de son bailleur actuel, de son employeur ou, cas échéant, d'une société de recouvrement, des informations à son sujet en relation avec la conclusion éventuelle d'un contrat de bail, en particulier des informations sur sa situation financière ? Oui Non (l'autorisation d'obtenir des renseignements de tiers est facultative, le demandeur pouvant y renoncer librement).»

i) Par demande du 6 décembre 2001, le PFPD a demandé à la présente Commission, en se fondant sur l'art. 29 al. 4 LPD, d'ordonner à la Société X de se conformer à sa Recommandation du 6 septembre 2001. Il fait valoir que la collecte de données à l'aide de la formule «Demande de location» constitue un traitement de données personnelles, que le fait que la personne concernée fournisse elle-même les données ne peut pas être considéré en l'espèce comme un consentement donné librement à une atteinte à la personnalité, qu'en particulier le consentement éventuel donné à la collecte de renseignements auprès de tiers n'est pas assez explicite et que la demande de certaines documents et de certaines informations est contraire au principe de proportionnalité.

j) Dans sa réponse du 11 février 2002, la Société X a contesté la compétence du PFPD pour émettre une Recommandation relative aux formules «Demande de location» car celles-ci sont signées par la personne concernée et constituent une offre de conclure un contrat de bail pour un logement donné au sens de l'art. 3 CO. Les formules ne peuvent donc, selon elle, présenter une «erreur de système» propre à porter atteinte à la personnalité d'un grand nombre de personnes. Selon la Société X, la présente Commission n'est dès lors pas non plus compétente pour rendre une décision au sens de l'art. 29 LPD. Sur le fond, la Société X considère que la personne concernée donne valablement son consentement au traitement des données contenues dans la formule et à la collecte de renseignements complémentaires auprès de tiers, de sorte que l'atteinte aux droits de la personnalité n'est pas illicite. Par ailleurs, la Société X considère qu'elle a, dans le cadre de démarches pouvant conduire à la conclusion d'un contrat de bail, un intérêt légitime prépondérant à obtenir les données en question, et cela indépendamment d'un consentement de la personne concernée.

k) Dans sa réplique du 5 juillet 2002, envoyée en traduction française le 5 septembre 2002, le PFPD fait d'abord remarquer que la formule de «Demande de location» du 21 décembre 2001 (pièce 13 du défendeur) est postérieure à la demande du 6 décembre 2001 adressée par lui à la présente Commission et ne peut donc pas être prise en considération. Le PFPD maintient ensuite que l'on est en présence d'une «erreur de système» pouvant porter atteinte à un nombre important de personnes et que la présente Commission est donc compétente pour prendre une décision au sens de l'art. 29 LPD. Il considère, sur le fond, que le consentement

donné par la personne concernée n'est pas valable car celle-ci est obligée de le donner si elle veut avoir la chance d'obtenir le logement qu'elle aimerait louer. Il rappelle en outre que la formule en question n'est pas remplie seulement par le futur locataire, mais par toutes les personnes qui s'intéressent au logement à louer. Il souligne enfin que l'existence d'un intérêt prépondérant au sens de l'art. 13 al. 2 LPD ne peut être admise que si le traitement de données respecte le principe de proportionnalité, ce qui n'est pas le cas pour certaines données demandées.

l) Dans sa duplique du 9 octobre 2002, la Société X se plaint d'abord du fait que le PFPD ait rendu publique l'existence de la présente procédure dans son rapport d'activité no 9 2001-2002 ainsi que du ton utilisé par le PFPD pour ce faire, tout en relevant que la présente Commission n'est pas compétente pour prendre d'éventuelles mesures à ce sujet. Elle demande que la formule «Demande de location» du 21 décembre 2001 soit prise en considération, dans la mesure où elle est la concrétisation d'engagements antérieurs pris par la Société X envers la PFPD; elle ajoute que, de toute façon, cette formule doit être prise en considération selon les principes de la procédure administrative. Elle maintient que l'objet de la présente procédure (demande de location) est différent de celui qui a donné lieu à la décision du 15 décembre 1995 de la présente Commission (listes d'attente), qu'il est d'ailleurs rare que le nombre de demandes de location pour un même logement soit supérieur à dix et que l'on ne peut pas parler d'«erreur de système» du seul fait que de nombreux logements sont mis en location. Au demeurant, la procédure de l'art. 29 LPD ne pourrait être mise en œuvre que si le traitement de données était illicite, ce qui n'est pas le cas car les données récoltées ne sont pas sensibles et que, de toute façon, leur traitement est licite en raison du consentement donné par la personne concernée et de l'intérêt prépondérant de la Société X.

m) Le PFPD comme la Société X ont renoncé à des débats publics.

II. DROIT

1. Selon l'art. 29 al. 4 LPD, le PFPD peut porter l'affaire devant la présente Commission lorsqu'une recommandation qu'il a émise au sens de l'art. 29 al. 3 LPD après avoir établi les faits selon l'art. 29 al. 1 et 2 LPD est rejetée ou n'est pas suivie. Il ressort ainsi clairement de cette disposition que la Commission n'a la compétence de statuer que si les faits se rapportent à l'une des situations énoncées à l'art. 29 al. 1 LPD (Décision de la présente Commission du 15 décembre 1995 [v. JAAC 62 no. 42 A], cons. II, 2, a). En l'espèce, il ne peut s'agir que de celle mentionnée à l'art. 29 al. 1 lit. a LPD (erreur de système).

2. Par «erreur de système», il faut entendre un système de traitement de données personnelles illicite quant au fond, en ce sens que le traitement est en soi agencé de manière à permettre la violation de la personnalité d'un grand nombre de personnes (Décision du 15 décembre 1995, cons. II, 2, b, cc). On doit donc être en présence 1° d'un système de traitement de données personnelles touchant un grand nombre de personnes et 2° d'un système de traitement illicite quant au fond.

3. Dans sa Décision du 21 novembre 1996 (v. JAAC 62 no 42 B), la présente Commission a statué sur la Recommandation émise le 21 novembre 1994 par le PFPD (Feuille fédérale 1994 V 407 ss), dans le cas particulier où cette Recommandation était adressée à la Rentenanstalt («Swiss Life»). La Recommandation en question visait d'une manière générale la récolte d'informations par le propriétaire ou la gérance de l'immeuble «en vue de permettre au bailleur de faire son choix entre plusieurs personnes intéressées au logement» (FF 1994 V p. 407). La Recommandation ne visait donc pas seulement les listes d'attente (pour lesquelles une disposition particulière était prévue au ch. 6), mais l'ensemble des formules d'inscription et autres informations personnelles que la personne intéressée par un logement peut être appelée à donner au bailleur (FF 1994 V p. 407). La Recommandation visait dès lors également le traitement de données en relation directe avec la conclusion du contrat de bail, en particulier celles concernant le cercle plus restreint des personnes entrant dans la sélection finale (FF 1994 V p. 408).

4. Dans sa Décision du 21 novembre 1996, la présente Commission a considéré que la demande du PFPD tendant à confirmer la dite Recommandation était, dans la mesure où elle était dirigée contre Swiss Life, recevable. Par là même, elle a admis que le traitement de données en vue de la conclusion de baux telle que décrit dans la Recommandation du 21 novembre 1994 constituait un système de traitement touchant un grand nombre de personnes au sens de l'art. 29 al. 1 lit. a LPD. Il n'y a pas lieu de revenir sur cette jurisprudence dans la présente espèce.

Certes, les formules dont il est question en l'espèce concernent la phase finale de sélection du locataire et donc, sans doute, un moins grand nombre de personnes que les simples listes d'attente. Il reste cependant que les formules en question seront utilisées en cas de relocation des milliers de logements dont la Société X a la gestion (plus de 35'000 selon une affirmation non contestée du PFPD) et que, dans chaque cas, elles concerneront plusieurs personnes (rarement plus de dix selon la Société X). Il ne fait donc pas de doute que les formules en question peuvent concerner un nombre important de personnes et que l'on est en présence d'un «système de traitement» de données personnelles au sens de l'art. 29 al. 1 lit. a LPD.

5. Il n'est pas contesté que les autres conditions de recevabilité fixées au cons. 3 de la Décision du 21 novembre 1996 de la présente Commission (le destinataire de la Recommandation est un bailleur ou agit pour lui, il a été entendu et a rejeté la Recommandation du PFPD) sont remplies en l'espèce. La demande du PFPD est donc recevable.

6. Pour que la Recommandation du PFPD soit justifiée quant au fond, il faut que le système de traitement analysé soit «susceptible de porter atteinte à la personnalité» de nombreuses personnes (art. 29 al. 1 lit. a LPD), c'est-à-dire qu'il soit illicite au vu des principes établis par la LPD.

   Selon l'art. 13 al. 1 LPD, une atteinte à la personnalité est «illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi». En l'espèce, il faut donc examiner si les personnes concernées par le traitement (les personnes intéressées par un logement) donnent un consentement valable à ce traitement et, si tel n'est pas le cas, si le traitement peut être justifié par un intérêt privé prépondérant de la Société X. Si aucun de ces motifs justificatifs ne devait être admis, il faudra encore examiner si le traitement constitue une atteinte à la personnalité; si tel est le cas, il devra alors être considéré comme illicite.

7. Les données directement récoltées par la formule de «Demande de location» sont fournies par la personne concernée elle-même. Ce faisant, elle consent à leur récolte. Pour que le consentement requis par l'art. 13 al. 1 LPD soit valable, il ne suffit cependant pas qu'il soit formellement donné ou, comme en l'espèce, qu'il résulte des circonstances. Il faut encore qu'il s'agisse d'un «consentement libre et éclairé», au sens de l'art. 27 CC, c'est-à-dire que la personne concernée puisse mesurer les conséquences de la décision qu'elle prend et qu'elle ait effectivement une liberté suffisante de ne pas consentir à l'atteinte. La validité du consentement s'apprécie au vu des circonstances du cas et, plus les données traitées portent atteinte à la personnalité, plus les exigences en ce qui concerne le consentement sont élevées (Décision de la présente Commission du 21 novembre 1996, cons. V, 1, b).

8. Dans le cas des personnes intéressées par un logement, la présente Commission a jugé que le consentement peut en principe être considéré comme valable si:

- les questions posées ne portent pas une atteinte excessive à la sphère privée (en particulier si elles ne sont pas compromettantes);
- le but des questions, en particulier leur relation avec la conclusion d'un contrat de bail, apparaît clairement;

- les caractéristiques du consentement sont indiquées; et
- le demandeur de logement n'est pas, de par l'état de contrainte dans lequel il se trouve, restreint dans sa liberté de faire ou de ne pas faire acte de candidature pour un logement donné, respectivement de répondre ou de ne pas répondre à certaines des questions posées (Décision du 21 novembre 1996, cons. V, 1, b.).

9. Au vu de ces critères, la présente Commission a jugé que la personne qui cherche un logement est, de par sa situation, restreinte dans sa liberté de refuser la collecte de certaines données en vue de la conclusion du bail. En outre, la situation économique de la personne, surtout pour celles de condition modeste, restreint le choix des logements possibles. A cela s'ajoute, lorsque le marché est tendu, la concurrence qui existe entre les candidats à un logement et qui place d'emblée celui qui refuserait de donner certains renseignements dans un position défavorable par rapport aux autres candidats. C'est pourquoi la présente Commission a, dans sa Décision du 21 novembre 1996 (cons. V, 1, b in fine) considéré que l'on ne peut pas admettre sans autre examen que le fait que les candidats à un logement aient donné eux-mêmes les renseignements demandés suffise pour que l'on puisse admettre qu'ils ont valable-ment consenti à l'atteinte.

10. Les arguments avancés par la Société X ne sont pas de nature à conduire la Commission à revenir sur cette appréciation. Il est vrai que la personne qui remplit une Demande de location pour un logement déterminé accepte de fournir les renseignements demandés et, normalement, mesure la portée des informations qu'elle fournit. Il est vrai aussi qu'elle n'est généralement pas dans un état de nécessité (il ne s'agit pas normalement d'un «sans abri», mais d'une personne qui possède déjà un logement). Il reste pourtant que le demandeur est face à un «système» (une formule de demande d'information) et que, s'il n'entre pas dans le système, il compromet ses chances d'obtenir le logement dès lors qu'il est en situation de concurrence avec d'autres demandeurs. Dans cette mesure, il existe bel et bien dans ce genre de situation un contexte qui restreint d'un point de vue pratique la liberté de décision du demandeur. On ne peut dès lors considérer qu'un consentement valable est d'emblée acquis et que, de ce fait, la collecte d'informations organisée par la formule de Demande de location est d'emblée licite selon l'art. 13 al. 1 LPD.

11. La formule de Demande de location utilisée par le Société X comporte en outre une demande de consentement spécial du demandeur à la récolte de renseignements auprès de tiers. Suite à l'intervention du PFPD, la Société X a plusieurs fois modifié la formulation de cette clause. La Commission a retenu le contenu de celle-ci tel qu'il est formulé dans la Demande de location du 21 décembre 2001

(voir ci-dessus I h). En effet, comme aucune règle de procédure ne prévoit le contraire, c'est l'état de fait tel qu'il se présente au moment où la décision est rendue qui est déterminant.

Dans sa teneur du 21 décembre 2001, la clause se présente comme une question, dont les termes ont été précisés quant aux tiers éventuellement interrogés et quant au contenu des renseignements demandés, avec en outre la précision que le demandeur peut librement renoncer à donner l'autorisation sollicitée. Telle qu'elle est désormais exprimée, cette clause permet effectivement au demandeur de donner un consente-ment «éclairé» à la Société X, car il peut mesurer quelle genre de renseignements vont être demandés aux tiers, et à quels tiers la Société X va s'adresser. En revanche, les remarques faites ci-dessus sur le caractère «libre» du consentement qui serait donné valent dans ce cas également. Car il est évident que le demandeur de loge-ment qui refuserait à la Société X le droit d'obtenir des renseignements auprès de tiers serait dans une situation défavorable en vue de l'obtention du logement.

12. Le consentement, tacite ou explicite, donné par la personne concernée ne peut donc pas, en l'espèce, être considéré comme un motif justificatif légitimant toute forme de récolte de données portant atteinte à la personnalité. Il faut dès lors examiner si la Société X peut faire état d'un intérêt privé prépondérant à recueillir, directement ou par l'intermédiaire de tiers, les informations qu'elle demande aux personnes intéressées par un logement.

L'art. 13 al. 2 lit. a LPD précise à ce sujet qu'un tel intérêt privé prépondérant entre notamment en considération si le «traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et [que] les données traitées concernent le cocontractant». Ce qui est donc décisif en l'espèce est de savoir si les données recueillies se rapportent au cocontractant, si elles sont directement utiles pour que le bailleur puisse prendre sa décision de conclure le bail, puis assurer l'exécution de celui-ci, et si l'intérêt du bailleur à disposer de ces données l'emporte sur celui du (futur) locataire à protéger sa personnalité. Cette analyse doit être faite séparément pour chacun des types de données pour lesquels la Société X n'a pas accepté la Recommandation du PFPD.

a) Point III 1.1. de la Recommandation: «souhaitant s'enquérir des conditions de logement actuelles du demandeur de logement, [la Société X] se cantonne à lui demander si son contrat de location a été résilié par le bailleur et si oui, pour quelle raison»

13. S'agissant du logement actuel, la formule de Demande de location comporte, outre les deux questions admises par la Recommandation, des questions sur la régie s'occupant de l'immeuble qu'habite le demandeur (facultatif), sur la date

depuis laquelle le demandeur est dans son logement actuel ainsi que sur le loyer mensuel (avec charges) payé par celui-ci (facultatif). Dans son rejet de la Recommandation, la Société X ne s'exprime que sur la deuxième de ces trois questions, qu'elle estime importante pour évaluer la stabilité du locataire.

Il est certes légitime pour un (futur) bailleur d'avoir des informations sur les problèmes importants qui ont pu survenir lors de l'exécution du bail en cours. Il suffit toutefois pour cela de connaître le motif pour lequel ce bail aurait été résilié. La durée du bail peut dépendre de facteurs qui n'ont rien à voir avec le bail lui-même (emploi du locataire, voire des membres de sa famille, cadre de vie, goûts du locataire ou de sa famille, etc.) et le (futur) bailleur n'a dès lors pas d'intérêt prépondérant à connaître cette durée. Le nom de la régie ainsi que le montant du loyer actuel ne sont pas nécessaires pour que le (futur) bailleur puisse prendre sa décision; pour les raisons indiquées plus haut, l'indication selon laquelle ces informations ne sont que facultatives ne suffit pas à en rendre la récolte licite. Pour les trois questions non autorisées par la Recommandation, le (futur) bailleur ne peut ainsi pas faire état d'un intérêt prépondérant.

b) Point III 1.2 de la Recommandation: «[la Société X] s'abstienne de réclamer à tout demandeur de logement son permis de séjour ou d'autres pièces de légitimation et qu'elle ne les réclame – pour autant qu'une disposition légale l'exige – qu'au demandeur qu'elle aura définitivement choisi»

14. Dans son rejet de la Recommandation, la Société X explique que le permis de séjour est très important pour déterminer la durée du bail. Il faut d'abord relever à cet égard que, selon le dernier état de la formule de Demande de location, la production du permis de séjour lui-même n'est exigée que de la part du locataire définitivement choisi et au moment de la signature du bail, ce qui est conforme à la Recommandation. La seule question qui demeure est donc celle de savoir si, préalablement, le bailleur peut s'informer sur le type de permis de séjour et la date d'échéance de celui-ci (qui n'est d'ailleurs pas demandée expressément dans la formule). On ne saurait nier que, pour choisir entre plusieurs locataires, la durée possible de leur séjour en Suisse est un élément important. L'intérêt du bailleur à connaître cette information, qui au demeurant n'est pas une donnée sensible, l'emporte dès lors sur celui du locataire à ne pas la donner.

15. S'agissant de la production d'autres pièces de légitimation au moment de la signature du contrat (livret de famille ou pièce d'identité pour les Suisses, etc.), la Société X indique dans son rejet de la Recommandation qu'il s'agit simplement de pouvoir contrôler auprès du locataire définitivement choisi les informations figurant dans le questionnaire qu'il a rempli.

Dès lors que la récolte des données comme telle est licite, il n'y a pas de raison de refuser que ces données puissent ensuite être vérifiées auprès du locataire définitivement choisi sur la base d'une pièce officielle (dont le but est justement de servir de légitimation des données en question). En ce sens, la production d'une pièce d'identité ou du livret de famille pour les Suisses, du permis d'établissement ou de séjour pour les étrangers ainsi que d'un certificat mensuel de salaire récent sont légitimes. (Pour l'attestation de non poursuites, voir ci-dessous 17.)

c) Point III 1.3 de la Recommandation: «[la Société X] s'enquière uniquement des poursuites pendantes dont le futur locataire fait l'objet depuis les deux dernières années»

16. Outre une question – conforme à la Recommandation – sur les poursuites pendantes durant les deux dernières années, la formule de Demande de location comporte une demande de renseignements sur d'éventuels actes de défaut de biens du demandeur (principe et, si oui, montant). Dans son rejet de la Recommandation, la Société X fait remarquer que toute personne justifiant d'un intérêt, dont un futur bailleur, peut demander ces informations aux offices de poursuites et de faillites et que cela simplifie les démarches si le demandeur de logement fournit lui-même l'information. Le PFPD ne conteste pas que ces informations peuvent être obtenues par le bailleur auprès des offices de poursuites et de faillites, mais estime qu'il est contraire au principe de proportionnalité d'exiger d'une personne, passé un certain temps, des informations sur la situation qui était alors la sienne.

Selon l'art. 2 al. 2 lit. d, la LPD ne s'applique pas aux données contenues dans les registres de poursuites et de faillites, dont la consultation est régie exclusivement par les art. 8 et 8a LP; ce sont ces dispositions qui garantissent la protection des données personnelles en la matière. Il faut en déduire que, aussi longtemps que les renseignements demandés se tiennent dans les limites des règles de la LP, la Société X a un intérêt prépondérant à les obtenir aussi directement de la personne concernée.

S'agissant des actes de défaut de biens, le questionnaire demande en réalité des informations concernant la situation financière actuelle du demandeur de logement, ce qui est légitime. Si ce dernier a entre temps désintéressé (intégralement ou partiellement) le créancier, l'acte de défaut de biens sera radié ou son montant sera réduit en conséquence (art. 149a et 150 LP). Si tel n'est pas le cas, l'acte de défaut de biens conserve son actualité. Mais la Société X ne peut pas demander plus d'informations que ce qu'elle pourrait obtenir en consultant les registres des offices de poursuites et de faillites. Or, le droit de consultation s'éteint après 5 ans (art. 8a al. 4 LP). Les renseignements demandés sur les actes de défaut de biens ne peuvent donc dépasser ce délai.

En résumé, dans la mesure où l'information peut de toute façon être obtenue auprès des autorités de poursuites ou de faillites et où elle vise la situation actuelle du demandeur de location, le bailleur a un intérêt prépondérant à demander directement l'information correspondante à la personne concernée; la demande de renseignements doit toutefois se limiter aux actes de défaut de biens des cinq dernières années.

17. La formule indique également que le locataire définitivement choisi devra produire au moment de la conclusion du bail une attestation de non poursuites délivrée par l'Office des poursuites. Contrairement aux autres pièces de légitimation demandées, qui ne sont requises que pour permettre la vérification des données, la production de cette attestation (et donc la preuve de l'absence de poursuites en cours au moment de la conclusion du bail) est une condition pour que le bail soit conclu («la signature du bail sera, dans tous les cas, subordonnée à la remise … [d'une] attestation de non poursuites»). Conformément à la Recommandation, cette attestation n'est demandée qu'à la personne qui a été définitivement choisie comme locataire. Comme indiqué plus haut, (le futur) bailleur a un intérêt prépondérant à obtenir cette attestation puisque le renseignement pourrait être obtenu directement par lui-même sur la base des art. 8 et 8a LP.

d) Point III 1.4 de la Recommandation: «[la Société X] renonce à exiger la déclaration de consentement proposée par elle au mois de juillet»

18. La formule du 21 décembre 2001 ne comporte plus la clause proposée en juillet 2001. La Recommandation est sur ce point respectée. Concernant ce point qui n'est de ce fait plus litigieux, la présente procédure devient sans objet

e) Point III 1.5 de la Recommandation: [la Société X] informe au préalable tout demandeur de logement qu'elle va requérir de tiers (sociétés et de recouvrement des créances, bailleur, employeur, etc.) des informations à son sujet et qu'elle lui donne la possibilité de refuser de l'y autoriser; à cet effet, le formulaire fera apparaître la rubrique correspondante, mentionnant que le demandeur peut l'autoriser à demander des renseignements sur son compte, mais qu'il n'y est pas tenu (caractère facultatif de l'autorisation)»

19. Dans son rejet de la Recommandation, la Société X a proposé une clause relative à ce consentement, clause qui est désormais reprise dans la formule de Demande de location du 21 décembre 2001. Cette clause est conforme à la Recommandation quant à la formulation de la question posée. Toutefois, le texte de la précision apportée entre parenthèses et en caractères gras sur le caractère facultatif de l'autorisation («l'autorisation d'obtenir les renseignements de tiers est facultative, le demandeur pouvant y renoncer librement») pourrait être plus clair, par exemple

dans le sens suivant: «L'octroi de cette autorisation est facultatif. Vous êtes libre de donner ou non l'autorisation demandée.»

Sous cette réserve, la clause proposée est conforme à la Recommandation.

Pour les raisons indiquées plus haut, le consentement de la personne concernée donné sous cette forme n'est cependant pas valable. La portée de la Recommandation est dès lors de reconnaître un intérêt légitime prépondérant à la Société X à recueillir ces données auprès de tiers, avec ou sans le consentement de la personne concernée. Mais, en acceptant la Recommandation sur ce point, la Société X renonce à exercer ce droit sans l'accord explicite du demandeur de logement, dans le sens d'un respect de la personnalité de celui-ci.

La Société X peut donc, lorsqu'elle y a été autorisée par la personne concernée, prendre auprès de tiers des renseignements en relation avec la conclusion éventuelle d'un contrat de bail. Ce faisant, la Société X veillera à respecter le principe de proportionnalité et à ne demander aux tiers que des informations qu'elle pourrait aussi obtenir de la personne concernée. Au demeurant, celle-ci aura toujours la possibilité – que le bail ait été conclu avec elle ou non – de vérifier en exerçant son droit d'accès quelles informations ont été données sur elle, et par quel tiers.

f) Point III 1.6 de la Recommandation: «[la Société X] ne peut exiger de documents supplémentaires du demandeur que si ces documents sont indispensables pour conclure le contrat de bail ou que la loi l'exige, et qu'elle ne pourra les exiger que du demandeur qu'elle aura définitivement choisi et uniquement au moment de signer le contrat. Elle ne pourra en exiger d'autres, sans rapport direct avec la conclusion du contrat de bail, qu'avec l'accord exprès de l'intéressé. Ici encore, le formulaire devra clairement faire apparaître le caractère facultatif de la fourniture de ces documents»

20. La formule de Demande de location n'exige pas la fourniture de pièces avant que l'un des demandeurs ait été choisi et que l'on prépare la signature du bail. Les documents à produire dans ce cas sont (sous réserve de l'attestation de non poursuites) destinés à permettre la vérification d'informations que la Société X est en droit de demander; le bien-fondé de leur production a été examiné plus haut et admis. Dans cette mesure, la Recommandation est respectée.

21. La Recommandation du PFPD telle qu'elle a été formulée au point III du document du 6 septembre 2001 ne comporte que les points énumérés ci-dessus. Seuls ces points ont donc formellement le caractère d'une décision qui peut être portée devant la présente Commission au sens de l'art. 29 al. 4 LPD. On remarquera que ces recommandations formelles ne recouvrent pas tous les points qui ont fait

précédemment l'objet de contestations. Ainsi, les questions sur les voitures/motos (y compris les numéros de plaques d'immatriculation) du demandeur de logement ainsi que sur son numéro de téléphone professionnel ne font pas l'objet d'une recommandation au sens formel. La Commission relève simplement que c'est à juste titre que le PFPD n'a pas insisté sur ces points. L'indication du numéro de téléphone professionnel n'a en effet qu'une simple portée pratique dès lors qu'il n'est pas contesté que la Société X peut demander des informations sur la profession et sur l'employeur du demandeur de logement. Quant aux informations sur la voiture (moto), elles sont utiles en vue de la location d'une place de parc correspondante, mais ne devraient effectivement être exigées que dans ce cas.

22. En résumé, la Commission constate que, parmi les points ayant fait l'objet d'une recommandation formelle de la part du PFPD, il y en a trois pour lesquels la Société X ne peut établir ni un consentement valable de la personne concernée, ni un intérêt privé prépondérant; ces points se rapportent aux demandes d'information sur la durée du bail actuel, le nom de la régie actuelle et le montant du loyer actuel. En outre, le caractère facultatif du consentement à obtenir certains renseignements auprès de tiers devrait être formulé plus clairement.

23. Sur les trois points mentionnés ci-dessus, la récolte de données par la Société X ne peut pas s'appuyer sur un motif justificatif. Pour que cette récolte soit illicite, il faut cependant encore qu'elle constitue une atteinte à la personnalité des personnes concernées.

A l'évidence, ces trois types de données ne sont pas des données rendues accessibles à tout un chacun au sens de l'art. 12 al. 3 LPD et dont le traitement n'est pas en règle générale, une atteinte à la personnalité. Les données sont au contraire visées par l'art. 12 al. 2 lit. a en relation avec l'art. 4 al. 2 LPD. Leur récolte porte atteinte à la personnalité des personnes concernées parce que ces données ne sont pas nécessaires pour que le (futur) bailleur puisse décider en connaissance de cause de la conclusion du bail; cette récolte est ainsi contraire au principe de la proportionnalité et elle constitue une atteinte à la personnalité des personnes concernées.

III. FRAIS

24. Selon l'art. 26 de l'Ordonnance concernant l'organisation et la procédure des commissions fédérales de recours et d'arbitrage, les frais de procédure sont fixés conformément à l'art. 63 PA et, exception faite de son art. 6 al. 2, conformément à l'Ordonnance du 10 septembre 1969 sur les frais et indemnités en procédure administrative.

D'après l'art. 63 al. 1 PA, les frais de procédure (émolument d'arrêté, émoluments de chancellerie et débours) sont en règle générale mis à la charge de la partie qui succombe. Si celle-ci n'est déboutée que partiellement, ces frais sont réduits. A titre exceptionnel, ils peuvent être entièrement remis. Le deuxième alinéa du même article dispose qu'aucun frais de procédure n'est mis à la charge des autorités inférieures, ni des autorités fédérales recourantes et déboutées.

En l'espèce, la formule du 21 décembre 2001 respecte finalement sur plusieurs points la Recommandation du PFPD; celle-ci a en outre été modifiée par la Commission sur quelques points. Dans cette mesure, les frais de la procédure devraient être mis à la charge du PFPD; toutefois, conformément à l'art. 63 al. 2 PA, le PFPD en tant qu'autorité fédérale ne supporte aucun frais.

Sur les questions touchant la durée du bail actuel, la régie de l'immeuble actuel et le montant de loyer actuel, la Commission a confirmé la Recommandation. La Société X succombe donc sur ces points et doit dès lors supporter une part des frais de procédure, arrêtée à 20 % de l'ensemble des frais. Les frais de procédure sont fixés à 2500 francs

25. En vertu de l'art. 64 al. 1 PA, il peut être alloué, d'office ou sur requête, à la partie ayant entièrement ou partiellement gain de cause une indemnité pour les frais indispensables et relativement élevés qui lui ont été occasionnés.

Conformément à l'art. 8 al. 2 de l'Ordonnance du 10 septembre 1969 sur les frais et indemnités en procédure administrative, les dépens doivent couvrir les frais suivants de la partie qui obtient gain de cause:

a) les frais de représentation ou d'assistance lorsque la personne qui représente ou assiste la partie au cours de la procédure ne se trouve pas dans un rapport de service avec elle;

b) les débours et autres frais de la partie en tant qu'ils dépassent 50 francs;

c) la perte de gain en tant qu'elle dépasse le gain d'une journée et que la partie qui obtient gain de cause se trouve dans une situation financière modeste.

Dans sa réponse du 11 février 2002, la Société X a conclu à l'allocation d'une indemnité de partie pour les frais indispensables et relativement élevés qui lui ont été occasionnés par la présente procédure. Si la Société X l'avait emporté sur tous les points, une indemnité de 5000 francs aurait été justifiée; comme la Société X succombe sur certains points, l'indemnité est réduite à 80 %, soit 4000 francs.

Pour ces motifs, la Commission arrête:

1. La Recommandation du 6 septembre 2001 du Préposé fédéral à la protection des données adressée à la Société X est confirmée en ce qui concerne le point III 1.1.
2. La formule «Demande de location du 21 décembre 2001 de la Société X respecte les points III.1.4, III.1.5 et III.1.6; la procédure engagée par le Préposé sur ces points est ainsi sans objet.
3. Le point III.1.2 de la Recommandation est modifié comme suit: «qu'elle ne demande des pièces de légitimation pour les données récoltées licitement que de la personne définitivement choisie comme locataire».
4. Le point III.1.3 de la Recommandation est modifié comme suit: «qu'elle s'enquière uniquement des poursuites pendantes dont le demandeur de logement fait l'objet depuis les deux dernières années et des actes de défaut de biens délivrés contre lui durant les cinq dernières années».
5. Les frais de procédure sont mis à la charge de la Société X à raison de 500 francs, le solde des frais n'étant pas perçu.
6. Une indemnité de partie de 4000 francs est allouée à la Société X.
7. Le jugement sera notifié aux parties.

Au nom de la Commission fédérale de la protection des données

Le Président: Le Secrétaire:

Voies de droit

Le présente décision est susceptible de recours de droit administratif auprès du Tribunal fédéral suisse dans les 30 jours suivant sa notification, conformément aux art. 97 ss. OJ. Le délai ne peut être prolongé. Le mémoire de recours, signé et annexant la présente décision, doit être adressé en triple exemplaire au Tribunal fédéral, Mon Repos, 1000 Lausanne 14.

13.9 Décision de la CFPD en matière de dépistage de la consommation de drogues auprès des apprentis

Voir paragraphe 13.9 de la partie en langue allemande.

13.10 Recommandations du PFPD

13.10.1 Recommandation du PFPD au sujet de la liste de licenciements d'Orange

Voir paragraphe 13.10.1 de la partie en langue allemande.