Préposé fédéral à la protection des données

Rapport d'activités 1995/96

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 1995 au 31 mars 1996.

TABLE DES MATIÈRES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

REPERTOIRE DES ABREVIATIONS

ADAK	Groupe de travail protection des données et liste des analyses / assurance-maladie
ADMAS	Registre des mesures administratives
AFIS	Système automatique d'identification des empreintes digitales
AUPER	Système d'enregistrement automatisé des personnes
AVS	Assurance vieillesse et survivants
BD	Banques des données
BVPLUS	Système de gestion informatisé du personnel (nouveau)
CFA	Caisse fédérale d'assurance
CFPD	Commission fédérale de la protection des données
CO	Code des obligations
DFJP	Département fédéral de justice et police
DOSIS	(Projet-pilote) Système provisoire de traitement des données en matière de drogue
FABER	Registre des autorisations de conduire
FMH	Fédération des Médecins Suisses FMH : Foederatio Medicorum Helveticorum
JAAC	Jurisprudence des autorités administratives de la Confédération
LPD	Loi fédérale sur la protection des données
MOFIS	Registre des véhicules et détenteurs
MP	Ministère Public
OCDE	Organisation de coopération et de développement économique
ODR	Office fédéral des réfugiés
OFP	Office fédéral de la police
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
PERIBU	Système de gestion informatisé du personnel
PFPD	Préposé fédéral à la protection des données
PIAS	Système de gestion et administration du personnel
PISEDI	Système de gestion du personnel du DFI
RCE	Registre central des étrangers
REGI	Gestion informatisée des personnes et des dossiers
RIPOL	Système de recherches informatisées de police
TED	Traitement électronique de données
ZAN	Index central des dossiers

I. THEMES CHOISIS

1. Affaires de police

1.1. Crime organisé - le système DOSIS

DOSIS est un système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants. Constitué sur la base d'un projet-pilote, DOSIS est géré par l'office central de lutte contre le trafic illicite de stupéfiants, au sein de l'Office fédéral de la police. Il a notamment pour fonction, par le biais d'un accès online, d'assurer la coopération avec les brigades des stupéfiants des corps de police des cantons. La phase d'essai externe limitée à huit cantons a été réglementée par l'intermédiaire d'une ordonnance provisoire du Conseil fédéral. Avec l'entrée en vigueur, le 15 mars 1995, de la loi fédérale sur les Offices centraux de police criminelle de la Confédération, le système DOSIS s'est vu doté d'une nouvelle base légale, applicable en particulier aux traitements de données personnelles. L'Office fédéral de la police a ensuite élaboré un projet de nouvelle ordonnance DOSIS et nous l'a soumis pour avis.

Donnant son aval à la proposition du Département fédéral de justice et police, le Conseil fédéral a soutenu la mise en fonction de la phase d'essai externe du système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants DOSIS. Conçu en tant qu'essai pilote et fondé sur une ordonnance provisoire, ce système informatique est géré par l'office central de lutte contre le trafic illicite de stupéfiants près l'Office fédéral de la police. Il a notamment pour but, par la mise en place d'un accès online, d'assurer la coopération avec les brigades des stupéfiants des corps de police des cantons.

Les travaux d'élaboration de cette ordonnance provisoire ont été effectués par l'Office fédéral de la police, avec notre collaboration. Outre le fait de limiter la phase d'essai externe à huit cantons, elle règle notamment les buts du système informatique DOSIS, ses sous-systèmes et les données traitées, les utilisateurs du système et leurs accès. Le traitement des données, à savoir en particulier leur saisie et le contrôle de leur qualité, leur communication, durées de conservation et effacement, ainsi que les mesures de sécurité, est également réglementé.

Parallèlement à cette phase d'essai externe du système DOSIS, est entrée en vigueur, le 15 mars 1995, la loi fédérale sur les offices centraux de police criminelle de la Confédération. Cette loi vise principalement à régler les tâches des office centraux de l'Office fédéral de la police dans leur lutte contre le crime organisé. Elle règle le détachement des agents de liaison à l'étranger, la collaboration avec les autorités de poursuite pénale et les services de police des cantons et de l'étranger ainsi que le traitement des données et les échanges nationaux et internationaux d'informations de police criminelle. Elle définit en outre les tâches de l'office central de lutte contre le crime organisé et de l'office central de lutte contre le trafic illicite des stupéfiants.

Avec l'entrée en vigueur de la loi fédérale sur les offices centraux, le système DOSIS s'est vu doté d'une nouvelle base légale, en particulier en ce qui concerne les aspects de traitement de données personnelles, nécessitant une adaptation de l'ordonnance provisoire.

Une première modification partielle de l'ordonnance a été effectuée le 15 mars 1995 déjà, afin d'y ancrer un renvoi aux dispositions d'exercice du droit d'accès de la loi

sur les offices centraux. En dépit des réserves que nous avions émises (cf. notre 2e rapport d'activités, p. 102 ss), une disposition légale spéciale dérogeant aux règles de la loi fédérale sur la protection des données a été adoptée, prévoyant un mécanisme de droit d'accès indirect à DOSIS.

Un projet de modification totale de l'ordonnance DOSIS destinée à réglementer le système définitif de traitement des données en matière de lutte contre le trafic illicite de stupéfiants a ensuite été élaboré par l'Office fédéral de la police. Ce dernier a tiré profit des enseignements tirés de la phase d'essai externe de DOSIS et des dispositions de traitement de données personnelles prévues dans la loi sur les offices centraux. Consultés sur ce projet, nous l'avons examiné sous l'angle de la protection des données, nous basant sur les informations et documents fournis, les résultats des séances de travail, ainsi que les démonstrations du système. Nous nous sommes en outre également efforcés de veiller à ce que d'une part, les dispositions proposées respectent le cadre légal imposé par la loi sur les offices centraux, et à ce que d'autre part, les nombreux traitements de données effectués dans le cadre de l'utilisation du système DOSIS soient clairement définis.

Différents points du projet d'ordonnance ont reçu notre aval. La disposition concernant les raccordements online des brigades des stupéfiants des corps de police des cantons et des collaborateurs de l'office central de lutte contre le trafic illicite de stupéfiants peut notamment être mentionnée. Nous avons par contre émis des réserves sur certains points du projet en soumettant à chaque fois une proposition concrète de solution. Ces points concernent en particulier l'élaboration d'évaluations spéciales et l'établissement de représentations graphiques, ainsi que la possibilité de marquer des éléments de comparaison avec des tierces personnes. Le mécanisme d'interrogation des sous-champs du système, les copies de certaines données de DOSIS dans l'index central des dossiers (ZAN) de l'Office fédéral de la police, ainsi que les durées de conservation des données et leur effacement ont également fait l'objet de réserves.

En outre, une divergence inhérente à l'interprétation d'une disposition particulière de la loi sur les offices centraux est à relever. Cette loi précise explicitement que dans le système de traitement des données, l'exploitation des informations recueillies avant l'ouverture d'une enquête de police judiciaire doit être effectuée séparément de celle des données de police judiciaire de la Confédération et des cantons. La concrétisation de cette norme au niveau du projet d'ordonnance est encore à l'examen, avec le concours de l'Office fédéral de la justice.

Enfin, nous avons exigé des explications sur le déroulement de la phase d'essai externe DOSIS. Nous avons en effet constaté que nous n'avions été ni informés ni consultés sur l'octroi d'autorisations d'accès au système à certaines polices cantonales pas mentionnées dans l'ordonnance provisoire et n'étant de ce fait pas autorisées à participer à cet essai pilote. Nous avons également relevé que la proposition au Conseil fédéral relative à l'adoption de la nouvelle ordonnance ne contenait, dans sa partie consacrée au déroulement de la phase d'essai externe, aucune mention de ces accès. Nous déplorons le fait de ne pas avoir été consultés et demandons que la proposition au Conseil fédéral, ainsi que le rapport final sur l'essai pilote DOSIS soient complétés en conséquence.

1.2. Blanchissage d'argent sale - Le projet de loi fédérale

Sur la base des résultats de la procédure de consultation (cf. notre 2e rapport d'activités, p. 108 ss), le Conseil fédéral a décidé que l'avant-projet de loi sur le blanchissage d'argent dans le secteur financier devait être totalement remanié. Nous avons salué cette décision dès lors qu'aucune disposition de protection des données n'avait été introduite dans cet avant-projet en dépit des nombreux traitements d'informations envisagés. Dans le cadre de l'élaboration du nouveau projet de loi, l'Administration fédérale des finances a rédigé des normes réglementant les traitements de données. Lors de l'examen de ces propositions internes, nous avons rappelé que des précisions doivent encore être apportées en ce qui concerne les traitements de données effectués par l'office central de lutte contre le crime organisé dans le cadre de l'application de cette loi.

Dans notre 2e rapport d'activités (p. 108 ss), nous avions souligné que, lors de la procédure de consultation relative à l'avant-projet de loi fédérale sur le blanchissage d'argent dans le secteur financier, l'attention de l'Administration fédérale des finances avait été attirée sur le fait que l'application d'une telle loi allait impliquer, pour les différents organismes concernés, un important travail de traitement de données. Toutefois, les questions de protection des données n'avaient pas été abordées par le groupe de travail interdépartemental au cours des travaux d'élaboration. Vu les incertitudes et options encore ouvertes, aucune réflexion relative aux aspects de protection des données n'avait été mentionnée dans le texte explicatif et aucune norme spécifique y relative n'avait été introduite dans l'avant-projet de loi.

Suite à la publication des résultats de la procédure de consultation, le Conseil fédéral avait décidé que cet avant-projet devait être totalement remanié.

L'Administration fédérale des finances nous a transmis pour avis en juillet 1995 un nouveau projet de loi encore à un stade d'élaboration interne. Constatant une fois encore qu'aucune norme de protection des données n'avait été introduite, nous avons réitéré nos propositions et observations en y apportant certains compléments. Aucune précision n'étant apportée dans ce projet, quant aux modes de transmission des données, nous avons insisté à nouveau sur le fait que si des échanges de données entre l'organe de communication, l'organe de contrôle ou des autorités cantonales, sont envisagés sous forme de procédure d'appel (liaisons online), une réglementation spécifique au niveau de la loi doit expressément le prévoir. Enfin, le projet renvoyant à la nouvelle loi sur les offices centraux de police criminelle de la Confédération entrée en vigueur le 15 mars 1995, nous avons signalé qu'une attention particulière doit être portée aux dispositions spéciales relatives au traitement de données personnelles qui y sont contenues, notamment aux normes à intégrer dans la loi sur le blanchissage d'argent et celles pouvant figurer dans une ordonnance.

En octobre 1995, une nouvelle version du projet de loi nous a été soumise, dans laquelle des dispositions sur le traitement des données personnelles ont été introduites. Ces dispositions, réunies dans une section spécifique de la loi, ont été élaborées sous forme de propositions par l'Administration fédérale des finances puis retravaillées avec notre collaboration. Prenant position en décembre 1995, nous avons confirmé que ces normes introduites dans la "section 6 : Traitement des données personnelles" constituent une bonne base de réglementation de l'imposant

travail de traitement des informations qu'implique l'application de cette loi pour les différents organismes concernés. Nous pensons ici en particulier aux collecte, enregistrement dans différents registres, conservation, communication et échanges de données personnelles, ainsi qu'aux restrictions à l'exercice du droit d'accès.

Nous avons toutefois rappelé que certaines précisions sont encore nécessaires, soit au niveau de la loi, soit de l'ordonnance. En outre, et c'est de notre point de vue la principale lacune de ce projet de loi, de nombreuses incertitudes demeurent encore en ce qui concerne les traitements de données qui seront effectués par l'autorité d'annonce ("Meldestelle"). Le projet de loi confie cette tâche à l'office central de lutte contre le crime organisé de l'Office fédéral de la police et renvoie ainsi à la loi fédérale sur les offices centraux de police criminelle de la Confédération. Le projet de message mentionne d'ailleurs que les modalités de gestion du futur système de traitement des données pour la lutte contre le blanchissage d'argent de l'Office fédéral de la police ne sont pas encore clairement définies. Nous avons dès lors demandé que le message précise comment cet office devra traiter les informations qui lui seront annoncées en application de la loi relative à la lutte contre le blanchissage d'argent. Ces précisions seront déterminantes en regard des normes qui devront encore y être intégrées et de celles qui pourront être élaborées au niveau de l'ordonnance d'application de la loi fédérale sur les Offices centraux de police criminelle de la Confédération.

Au stade actuel du projet, et en accord avec l'Administration fédérale des finances, nous n'avons pas émis d'autres commentaires, considérant ces dispositions comme un premier jet, fruit de la collaboration entre nos services respectifs. Nous examinerons l'ensemble du projet lors de la procédure de consultation qui sera ouverte dans le courant de 1996. Il nous sera alors possible de nous prononcer définitivement, en particulier quant aux traitements de données qui seront effectués par l'office central de lutte contre le crime organisé dans le cadre de l'application de cette loi et aux conséquences législatives en découlant.

1.3. Sûreté intérieure - les débats parlementaires

Après avoir été traité en plenum du Conseil des Etats le 13 juin 1995, le projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure a été transmis à la Commission des affaires juridiques du Conseil national. Ce projet de loi renferme de nombreux aspects problématiques du point de vue de la protection des données. Nous avons ainsi notamment pris position de manière critique sur les dispositions concernant l'exercice du droit d'accès et la recherche spéciale d'informations permettant l'usage d'appareils techniques de surveillance.

Le projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure élaboré par le Conseil fédéral en mars 1994 est actuellement débattu devant le Parlement. Consultés sur l'avant-projet de loi, nous avions émis un certain nombre de réserves et propositions. Lors des discussions échangées en Commission des affaires juridiques du Conseil des Etats, nous avons eu l'occasion de nous prononcer en particulier sur la disposition consacrée à l'exercice du droit d'accès des personnes concernées.

En séance plénière du 13 juin 1995, le Conseil des Etats a, en dépit de nos réserves, décidé de suivre la proposition de sa Commission, en introduisant dans le projet

de loi une disposition relative au droit d'accès similaire à celle adoptée dans la loi fédérale sur les offices centraux de police criminelle de la Confédération entrée en vigueur le 15 mars 1995. Lors de cette même séance, il a également accepté d'introduire un nouvel article concernant la recherche d'informations spéciales. Cette norme vise en particulier à permettre, dans le domaine de la police préventive, la surveillance de la correspondance postale et des télécommunications ainsi que l'utilisation d'appareils techniques de surveillance.

Auditionnés par la Commission des affaires juridiques du Conseil national en octobre 1995, nous avons mis en évidence les dangers inhérents à l'introduction d'une telle disposition. Ses conditions d'utilisation, beaucoup trop larges par rapport à ce que prévoit la procédure pénale, ont été considérées comme critiques, ainsi que son application au domaine de la police préventive. En janvier 1996, la Commission a décidé de ne pas suivre le Conseil des Etats et a biffé cette norme. La Commission avait en outre préalablement décidé en novembre 1995 de biffer également la notion de crime organisé, estimant que cette tâche ne relève pas de la sûreté intérieure.

Eu égard aux nombreux aspects de protection des données inhérents à ce projet de loi, nous avons été invités à participer à la séance de la Commission des affaires juridiques du Conseil national prévue pour février 1996. Ce projet sera ensuite traité en séance plénière du Conseil national.

1.4. Le système automatique d'identification des empreintes digitales AFIS

Du fait des développements survenus dans le domaine de l'identification des personnes, il s'est avéré inévitable de restructurer la section Identification de l'ODR et la section Service d'identification de l'OFP. Le nouveau concept Service AFIS prévoit une seule unité de traitement pour toutes les prestations d'AFIS. Le Service AFIS se chargera notamment de l'identification des empreintes digitales et de la communication de brèves fiches signalétiques. Les compétences spécifiques à l'ODR et à l'OFP demeureront séparées.

Le système AFIS a pour but l'identification de personnes à partir d'empreintes digitales. Il constitue une banque de données d'empreintes digitales commune aux domaines de la police et de l'asile. AFIS soulève la question de sa conformité avec le principe fondamental du droit de la protection des données, à savoir celui de finalité. A l'occasion de la première étape de réalisation, nous avons examiné le projet Service AFIS à la lumière du principe que nous venons de mentionner. Nous avons établi qu'il convenait de veiller à la séparation des données de police de celles relevant de l'asile lors de la réalisation du projet et dans les modifications de loi prévues, tant du point de vue structurel que des autorisations d'accès de l'OFP et de l'ODR. Nous avons en particulier souligné la nécessité de peser les intérêts en jeu avant de communiquer au secteur policier des données concernant les réfugiés. Ainsi de brèves fiches signalétiques de réfugiés ne peuvent être communiquées au secteur policier qu'en présence d'un motif de police suffisant. La communication d'une identité effectuée de cette manière ne peut être transmise à l'étranger qu'avec l'accord de l'ODR ou des autorités chargées de mandats en vertu de la loi sur l'asile. Cette solution tient compte en particulier de l'interdiction, posée par le droit d'asile, de communiquer à l'étranger des données concernant les réfugiés. Elle est également valable pour le système Rapid Response AFIS. Une plus large

communication de données ne peut avoir lieu qu'à titre d'entraide administrative et après une pesée approfondie des intérêts en jeu.

La discussion portait également sur la possibilité d'étendre le système Rapid Response AFIS (RRA) à d'autres cantons. RRA est un système d'identification des empreintes digitales dont dispose le canton de Zurich en raison de sa situation spéciale en matière de drogue. Il se caractérise par une communication de la brève fiche signalétique et de son titulaire. A part cela, il ne se distingue guère du reste du système AFIS. Il est notamment soumis aux mêmes règles du droit de la protection des données. RRA constitue en tant que tel un modèle pour le projet Service AFIS. Nous avons fait dépendre l'intégration d'autres cantons dans le système RRA de la création d'une base légale au niveau d'une ordonnance du Conseil fédéral.

1.5. Automatisation du casier judiciaire VOSTRA

Le projet d'automatisation du casier judiciaire VOSTRA est réparti entre diverses unités de réalisation et sera développé par étapes entre 1996 et 1998. La création d'une base légale au sens formel est prévue au plus tôt pour 1998. Il est impossible pour des raisons de protection des données de créer une ordonnance transitoire qui servirait de base légale pour la période 1996-1998.

Le projet VOSTRA a pour but d'automatiser la gestion des extraits de jugements et des extraits du casier judiciaire à l'Office fédéral de la police. Il transpose, du papier aux supports électroniques, l'échange de données avec d'autres services fédéraux et cantonaux. La première étape de réalisation consiste essentiellement à communiquer, par procédure d'appel (online), l'extrait du casier judiciaire d'une personne sans indication des peines. La deuxième étape prévoit la communication online de l'extrait de casier judiciaire, peines comprises. La réalisation progressive de ces étapes aura lieu en majeure partie avant 1998, alors que la réglementation dans le code pénal n'est prévue que pour 1998. La réalisation du système sur la base d'une ordonnance transitoire est impossible, car le droit de la protection des données requiert une base légale au sens formel. Il faut donc créer la base légale requise pour le traitement des données du casier judiciaire et leur communication.

1.6. Révision de la loi sur la circulation routière

Une série d'interventions parlementaires a mené à la nécessité de réviser la loi sur la circulation routière. Dans le cadre de la consultation des offices, nous avons fait part de nos préoccupations relevant du droit de la protection des données, essentiellement quant à la densité de réglementation. Nous avons en outre proposé de ne pas publier le registre des détenteurs de véhicules. Une initiative parlementaire va d'ailleurs dans le même sens.

Dans le domaine de la circulation routière, la Confédération est appelée à gérer divers systèmes automatisés de traitement des données. Il s'agit ici d'une part du registre des mesures administratives ADMAS, du registre des permis de conduire FABER, du registre des véhicules et des détenteurs de véhicules MOFIS, d'autre part du registre concernant la statistique des accidents. Ces registres contiennent en partie des données sensibles. Il convient donc, en cas d'automatisation du traitement, de soumettre les bases légales à des critères stricts. A l'occasion de la

consultation des offices, nous avons constaté une densité de réglementation insuffisante des bases légales en question. Ces bases doivent réglementer notamment, et avec un degré de précision suffisant, le but du traitement des données, les autorités habilitées à effectuer le traitement et leurs tâches, les destinataires des données, les moyens utilisés, le cercle des personnes concernées, les données personnelles traitées, la transmission des données et la protection contre les abus.

Afin d'atténuer les risques d'atteinte à la personnalité, nous avons en outre proposé dans le cadre de la consultation des offices de renoncer à la publication du registre des détenteurs de véhicules. Cela doit notamment empêcher que des informations relatives aux détenteurs de véhicules parviennent dans des canaux d'information publics. Une initiative similaire a été également déposée au niveau parlementaire. Elle est actuellement examinée par les Commissions des affaires juridiques du Conseil national.

2. Droit des étrangers et droit d'asile

2.1. Accès des postes de police au Registre central des étrangers RCE

Dans un recours à la Commission fédérale de la protection des données, nous avons critiqué les problèmes non encore résolus de l'accès des postes de police au RCE et du traitement des données de ce registre au moyen de la bureautique. Il s'agit en effet de limiter dans une mesure raisonnable l'accès de la police et de relier les systèmes d'automatisation bureautique en une configuration conforme à la LPD.

Nous avons tout d'abord soumis à la CFPD la question de savoir si le recours à la bureautique par l'Office fédéral de la police (OFP) garantissait un traitement sûr et confidentiel des données relatives aux étrangers. Ces données, dont l'accès est ouvert à l'OFP, ne peuvent pas être combinées avec les données de recherche judiciaire de l'OFP pour constituer de nouveaux enregistrements ou fichiers, ni être comparées avec les fichiers de recherche judiciaire de l'OFP. Elles ne peuvent pas non plus être communiquées sans autorisation à des tiers en Suisse ou à l'étranger (voir aussi à ce sujet nos 1er et 2ème rapports d'activités p. 107 ss et p. 112 ss). A nos yeux, les mesures de sécurité appliquées jusqu'ici à l'OFP ne présentent pas une garantie suffisante pour exclure les fausses manipulations et les pannes, ou au moins pour rendre improbable l'accès non autorisé. L'évaluation des risques décrite dans l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, et que devraient respecter les spécialistes de la sécurité de l'Office fédéral de l'informatique doit encore être effectuée. Au vu des possibilités techniques de traitement à disposition, nous avons estimé qu'une simple interdiction de traitement était insuffisante et exigé que les applications elles-mêmes soient dotées de mesures de sécurité tout à fait possibles aujourd'hui et correspondant aux standards internationaux.

Il s'agissait ensuite de savoir si et à quelles conditions on pouvait rendre accessibles, par procédure d'appel, aux différents organes de l'OFP chargés en partie de tâches de recherche judiciaire, les données du RCE collectées à des fins civiles. Nous considérons que la protection suffisante de ces données est une première condition

sine qua non. Mais malgré nos sommations répétées, nous n'avons pas ou pas suffisamment reçu cette assurance. La deuxième condition impérative pour la mise en place d'une procédure d'appel est que cette procédure soit vraiment indispensable dans le cas concret à l'accomplissement des tâches, et que d'autres formes moins incisives de communication de données, en cas d'entraide administrative, soient insuffisantes. Il ressort d'une analyse interne auprès de l'OFP que seul un petit nombre d'organes de cette autorité disposant d'une liaison en ligne au RCE les utilise fréquemment. Pour ces quelques consultations par jour ou par semaine, des transmissions de données de cas en cas (par le biais informatique) suffiraient la plupart du temps. Du point de vue de la protection des données, les transferts de données online qui ont lieu selon le "principe du self-service" et sans pesée préalable des intérêts doivent être considérés comme incisifs, notamment dans le domaine délicat de la police. Il faut les éviter partout où c'est possible. Cela ressort du principe de la proportionnalité et - compte tenu d'une éventuelle discrimination des étrangers par rapport aux Suisses dans le domaine de l'information - ainsi que de l'obligation d'égalité de traitement. Des autorités et des tribunaux étrangers traitent également des questions similaires, notamment le tribunal constitutionnel allemand.

2.2. Révision partielle restreinte de l'ordonnance sur le RCE

La révision partielle restreinte de l'ordonnance sur le RCE a tenu compte des circonstances actuelles, en ce sens que les noms des parents nourriciers d'enfants étrangers doivent aussi être saisis dans le RCE pendant une courte période transitoire. En outre, les données des réfugiés transmises au RCE pour l'impression d'un passeport ne peuvent pas être enregistrées dans le RCE.

Lorsque les noms des enfants sont connus, les noms des parents nourriciers doivent être effacés, de même que les noms des enfants au plus tard un mois après leur adoption. A cette occasion, le Conseil fédéral a aussi fixé que *les données personnelles de l'AUPER* transmises au RCE par l'Office fédéral des réfugiés pour l'impression des passeports *ne devaient pas être enregistrées dans le RCE*. Dans ce contexte, le Conseil fédéral nous a suivis. Le principe de finalité s'opposerait aussi clairement à une réunion même partielle des données des requérants d'asile et des autres données relatives aux étrangers. Ajoutons à cela que les données sensibles des requérants d'asile imposent à un fichier des exigences très sévères en matière de sécurité; lors d'une combinaison même partielle avec un autre fichier, lesdites exigences seraient "transmises en héritage" à cet autre fichier. En raison de la structure ramifiée et de l'importance du RCE, d'autres problèmes importants surgiraient pour ce genre de fichier.

2.3. Suisses et Suissesses dans le Registre central des étrangers

Des personnes privées nous ont demandé si les données des Suisses et des Suissesses enregistrées dans le Registre central des étrangers RCE pouvaient également être consultées par le système de recherche RIPOL.

Selon l'ordonnance sur le RCE, les employeurs suisses (des entreprises pour la plupart) de travailleurs étrangers sont souvent enregistrés dans le RCE; il en va de même pour les hôtes suisses ainsi que, durant une période transitoire de deux ans,

pour les personnes nouvellement naturalisées suisses. S'y ajoutent encore, comme mentionné précédemment, les parents nourriciers d'enfants étrangers. Par la ligne RIPOL, les autorités policières et douanières ne peuvent consulter dans le RCE qu'un champ restreint de données qui doivent être associées au nom d'un étranger. Il est vrai que l'on trouve ici également les champs de données "employeur" et "adresse" des étrangers. L'accès à "l'hôte" helvétique n'est par contre ouvert qu'à l'Office fédéral des étrangers, au service des recours du DFJP, aux représentations suisses à l'étranger ainsi qu'aux autorités cantonales de police des étrangers, mais pas à la police. Quant au champ de données "parents nourriciers" du RCE, il ne peut pas non plus être consulté par la ligne RIPOL. A ce sujet, il est en outre prévu de limiter l'accès des autorités cantonales compétentes (en règle générale la police des étrangers) aux parents nourriciers établis dans leur canton, ce qui, du point de vue de la protection des données, devrait s'effectuer rapidement. Le cryptage, dans un domaine sensible comme l'adoption, devrait indiscutablement améliorer le respect de la confidentialité.

Ainsi, seules les données des personnes naturalisées suisses depuis moins de deux ans et des employeurs suisses de ressortissants étrangers peuvent être consultées par la police, respectivement par la ligne RIPOL dans le RCE. Il ressort toutefois de nos investigations que les personnes nouvellement naturalisées suisses figurent dans le RCE parfois plus longtemps que la durée admise de deux ans. Les organes compétents du DFJP ont maintenant effacé du RCE les données des personnes naturalisées depuis plus de deux ans dans notre pays. En outre, pour l'heure on ne peut pas empêcher par des moyens techniques d'introduire dans le champ de données "adresse" du RCE *les hôtes suisses à la place des personnes étrangères accueillies*. On ne peut donc pas exclure avec certitude que des données relatives à des hôtes suisses de ressortissants étrangers soient, selon les circonstances, communiquées sous le champ "adresse" aux autorités policières par le biais de la ligne RIPOL, même si cela est contraire à l'ordonnance sur le RCE. Il est évident que pour le moment, il n'existe pas de procédure (électronique) efficace - contrairement à ce qui se passe pour les personnes nouvellement naturalisées - qui permette d'effectuer dans le RCE des contrôles ultérieurs de saisies erronées de Suisses et de Suissesses. Dans une circulaire, l'Office fédéral des étrangers a bien sûr attiré l'attention des autorités cantonales compétentes sur la situation juridique et leur a rappelé leur devoir de discrétion. Nous estimons toutefois qu'il faut impérativement aussi installer dans le RCE *des procédures de contrôles efficaces* comme le prescrit expressément l'ordonnance relative à la loi fédérale sur la protection des données dans les dispositions relatives au règlement de traitement. C'est pourquoi il faut accorder aux contrôles l'attention nécessaire dans le cadre de l'édiction d'un règlement de traitement du RCE. Nous restons en contact avec l'Office fédéral des étrangers et nous réservons le cas échéant le droit d'édicter une recommandation adéquate.

2.4. Nombre maximum de danseuses par établissement

Afin de renforcer la lutte contre les abus lors de l'engagement de danseuses étrangères, il a été mis à disposition des autorités cantonales de police des étrangers la nouvelle fonction "Nombre maximum de danseuses par établissement" dans le Registre central des étrangers RCE.

Aussi longtemps qu'il n'y a pas communication de données personnelles, aucune adaptation de l'ordonnance sur le RCE n'est nécessaire. Nous avons accepté l'introduction de la fonction précitée. Par la même occasion, nous avons relevé qu'une fonction sur la consultation online de "Listes nominatives de tous les étrangers par exploitation" n'était pas licite sans adaptation préalable de l'ordonnance sur le RCE. En outre, il faudrait prendre des mesures techniques de protection au cas où une introduction générale de ce genre de traitement de données approfondi ne semblerait pas d'emblée anticonstitutionnelle (voir à ce sujet le rapport relatif à notre recours auprès de la CFPD p. 143).

2.5. Recherches dans le RCE

Dans de nombreux cas, les autorités désireuses d'accéder au Registre central des étrangers disposent de données précises sur la personne concernée. Dès lors, une procédure de recherche dans le RCE est inutile.

Tel est par exemple le cas lorsqu'une autorisation de séjour doit être prolongée et que la désignation de la personne peut être effectuée sur la base du dossier. Dans d'autres cas, lorsque l'autorité qui effectue la recherche n'a pas le dossier ou lorsqu'aucune pièce d'identité ne peut être présentée, il faut travailler avec les indications disponibles qui ne sont pas toujours très précises. A cet effet, le RCE a son propre instrument qui, sur la base de critères de recherche et de questions multiples gérées par ordinateur, permet de rechercher à l'écran les données d'un choix de personnes éventuellement concernées par les indications. On peut bien sûr consulter d'autres données sur les personnes concernées, ce qui permet d'établir un classement plus précis.

Lors de la présentation de cette fonction, nous avons constaté que les critères de recherche à disposition étaient en partie saisis d'une manière extraordinairement étendue, ouvrant ainsi la voie à la consultation d'un éventail de personnes beaucoup trop large. C'est pourquoi nous avons exigé des restrictions substantielles à cette fonction de recherche, restrictions que l'on nous a promis d'introduire. D'une manière générale, il s'agit de définir des critères de recherche les plus précis possibles à l'intention des autorités qui consultent le RCE sur la base de critères de reconnaissance de personnes ne figurant pas clairement et nettement dans leurs dossiers. Dans ce cadre, il faut éliminer les combinaisons de recherches susceptibles de léser la personnalité même si, dans certains cas, elles s'avèrent éventuellement plus précises que d'autres. En ce qui concerne les consultations du RCE par la police via la ligne RIPOL, nous n'avons trouvé aucune combinaison pouvant léser la personnalité.

2.6. Directives provisoires relatives à la journalisation dans le RCE

Si, dans un traitement déterminé, les mesures préventives ne suffisent pas à exclure avec suffisamment de sécurité des détournements du principe de finalité, les traitements de données doivent faire l'objet d'une journalisation.

Cette directive correspond aux exigences de sécurité reconnues sur le plan international et est prescrite par l'article 10 OLPD. Pour sa mise en application, le DFJP a édicté le 2 novembre 1994 des "Directives provisoires sur la journalisation de la

consultation des données du Registre central des étrangers au moyen d'une procédure d'appel". Sur cette base, les transmissions de données par le RCE au moyen du masque de consultation du RIPOL doivent être journalisées. La désignation de l'office, l'utilisateur et le numéro d'utilisateur, la date et l'heure de la consultation ainsi que les critères de recherche utilisés doivent être protocolés. Le centre de calcul du DFJP met à disposition un programme d'évaluation pour le fichier de journalisation et enregistre les données de journalisation pendant une année. Les conseillers à la protection des données du DFJP contrôlent régulièrement ces protocoles, vérifiant notamment si les différentes consultations sont nécessaires à l'exécution d'une tâche légale et si les données de tiers non concernés continuent à être utilisées. Ils établissent une fois par année un rapport à l'intention du Secrétariat général.

Du point de vue de la protection des données, ces directives sont louables. Il reste maintenant à les transposer définitivement, tout en profitant de l'occasion offerte pour y introduire toutes les adaptations qui s'imposent actuellement. Des prescriptions relatives à la protection des collaborateurs font notamment défaut, ce qui pourrait diminuer le taux d'acceptation des directives. Il faudrait également introduire quelques critères d'évaluation supplémentaires afin de donner suite avec plus d'efficacité au mandat légal. Lors de présentations successives des journalisations au centre de calcul du DFJP, il s'est en outre avéré que l'évaluation avec les moyens disponibles jusqu'ici prenait beaucoup de temps et était ardue. Les solutions standard que l'on peut facilement obtenir aujourd'hui, voire les ressources déjà disponibles dans les logiciels de l'exploitation concernée ne sont pas ou que peu utilisées. Nous allons soumettre des propositions concrètes aux organes compétents du DFJP.

2.7. Système de gestion sans papier des dossiers de personnes REGI-2

Des exigences importantes de protection des données ont été remplies au niveau du système de gestion sans papier des dossiers de personnes REGI-2 de l'OFE. Les documents sont mémorisés sans possibilité de modification ultérieure. La recherche de textes complets n'est pas possible. La réglementation des accès est effectuée par des index standardisés qui permettent aussi la recherche de documents séparés. Un règlement de traitement a été émis. Il reste toutefois encore plusieurs problèmes non réglés en matière de protection des données, à résoudre le plus rapidement possible.

Suite à nos recommandations (voir notre 2e rapport d'activités p. 116 ss), l'Office fédéral des étrangers a présenté pour ce nouveau système TED un règlement de traitement accompagné de la documentation y relative. Pour l'essentiel, il ressort de ces documents que le REGI-2 sert à l'archivage sans papier des dossiers personnels traités par cet office. Dans ce contexte, les différents documents sont mémorisés de manière à empêcher toute modification et recherches de textes complets. Un champ d'index, fixé d'après un standard prédéfini, figure ainsi sur ces documents. Il permet de trouver rapidement le document intéressant, tout en autorisant, à l'aide de moyens informatiques, un accès, respectivement une communication à des tiers selon leurs tâches. Les traitements de données sont journalisés.

La solution choisie répond à de nombreuses exigences de protection des données, même s'il faut encore résoudre certains problèmes. Ainsi, il n'est pas encore clairement défini comment, par qui et selon quelle procédure les contrôles

périodiques internes à l'office prescrits dans l'OLPD seront effectués. De même, il semble que jusqu'ici, aucune évaluation des risques n'a été entreprise, alors même qu'au vu des données sensibles et des profils de la personnalité qui sont traités, elle est pourtant légalement prescrite. Selon l'ordonnance concernant la protection des applications et des systèmes informatiques dans l'administration fédérale, il faut associer à cette évaluation des risques les spécialistes de la sécurité informatique de l'administration fédérale. Comme les résultats de cette analyse peuvent aussi être importants pour la protection des données (catalogue des mesures), des éléments essentiels à une évaluation globale nous font défaut. C'est pourquoi nous n'avons pu jusqu'ici nous exprimer que sur des questions formelles (intégralité du règlement de traitement et des documents exigés par l'OLPD).

2.8. Registre automatisé des personnes AUPER-2

Dans un recours auprès de la CFPD, nous avons - comme pour le RCE - critiqué les problèmes non résolus lors de l'accès des postes de police aux données des requérants d'asile figurant dans l'AUPER et du traitement de ces données par bureautique. Il s'agit de réduire dans une mesure raisonnable l'accès de la police et d'intégrer les systèmes bureautiques dans une architecture de sécurité conforme à la LPD. Il est inadmissible de voir qu'aujourd'hui encore, les données de l'Office fédéral des réfugiés sur les requérants d'asile et des données importantes de l'Office fédéral de la police sont enregistrées dans une seule et même banque de données de l'AUPER. Indépendamment de ce recours, nous avons indiqué qu'il fallait, dans le cadre de la gestion des comptes des requérants d'asile par les PTT, séparer clairement les autres traitements de données et garantir la sécurité des données des requérants d'asile.

Pour l'AUPER-2 également (comme pour le RCE, voir ci-dessus p. 122), nous avons posé à la CFPD la question de l'engagement de moyens bureautiques dans le respect de la confidentialité des données de l'asile. Cette question se pose de manière encore plus aiguë pour l'AUPER-2 que pour le Registre central des étrangers RCE. D'une part, il s'agit également, en garantissant le traitement confidentiel des données de l'asile, de respecter des obligations de droit public. Les requérants d'asile dans notre pays ne devraient pas être exposés à des inconvénients supplémentaires dûs à des pannes en matière d'information. Il est impossible d'exclure ces pannes informatiques dans un système aussi ramifié que l'AUPER, si l'on n'a pas fourni les efforts requis pour un traitement de données contrôlé et sûr sur tous les plans.

Du point de vue du droit de la procédure, il s'agit en outre d'éviter des raisons de fuites ultérieures. Celles-ci peuvent survenir lorsque des informations sont communiquées sur une personne, augmentant de ce fait sensiblement la probabilité d'une persécution dans le pays d'origine de la personne concernée. Si, dans certains cas, d'autres autorités que les autorités d'asile se voient octroyer des accès online pour les données de l'asile parce que ces accès se révèlent absolument nécessaires à la résolution de leurs tâches, il faut leur interdire de transmettre plus loin les données ainsi obtenues et garantir le respect de cette interdiction par des mesures techniques. En outre, il faut limiter dans une mesure raisonnable les procédures de recherche.

Les traitements de données doivent être considérés comme disproportionnés si, dans le cadre de la méthode de traitement choisie, l'on accepte d'emblée de "cotraiter" les données d'un grand nombre de tiers non concernés lors de chaque traitement, d'autant plus si on peut l'éviter par un volume de travail acceptable. La fonction de recherche installée aujourd'hui dans l'AUPER-2 au profit des organes de police de la Confédération (mais aussi des cantons) ne répond pas aux exigences de la LPD.

Notre allégation auprès de la CFPD, selon laquelle les données de l'asile enregistrées dans l'AUPER-2 doivent être séparées des données de police de l'Office fédéral de la police (OFP) enregistrées dans le même fichier (ce qui n'est malheureusement toujours pas le cas), allait dans le même sens (voir aussi nos 1er, p. 107 ss et 109 ss et 2ème rapports d'activités, p. 117 ss). Aujourd'hui, lorsqu'un employé de l'OFP consulte les données de police de l'OFP dans l'AUPER-2, il obtient parfois également un nombre indéterminé de données d'asile même s'il ne les désire pas expressément, ce qui est absolument insoutenable. Nous avons une fois de plus signalé avec toute l'insistance voulue que cette regrettable faute dans le système devait être corrigée au plus vite. Reste à espérer que la procédure pendante auprès de la CPFD, ainsi que l'évaluation des risques des traitements de données, effectuée en parallèle au sein de l'ODR et de l'OFP, en collaboration avec l'OFI et une université suisse, déboucheront sur une solution conforme à la protection des données. Il faut aussi *associer le centre de calcul du DFJP,* qui doit créer sur une large échelle les conditions pour une solution conforme au droit de la protection des données.

2.9. Compte des prestations de sécurité des requérants d'asile "Compte de sécurité"

Selon l'ordonnance 2 sur l'asile, les requérants d'asile ont l'obligation de déposer sur un compte une quote-part déterminée de leur revenu professionnel en Suisse afin de garantir d'éventuelles prestations d'assistance ou des mesures de rapatriement; ce genre de compte est actuellement géré par l'entreprise des PTT en collaboration avec l'Office fédéral des réfugiés (ODR). Il en résulte de nombreux flux de données entre les deux organes fédéraux.

Dans une recommandation nous avons exigé la mise en place d'un concept global de sécurité accompagné d'un catalogue de mesures appropriées pour l'échange et le traitement des données sensibles des requérants d'asile par les PTT, ainsi qu'un règlement de traitement répondant aux exigences de l'OLPD. De surcroît, nous avons exigé que les données délicates des requérants d'asile soient transmises sous forme chiffrée et traitées par les PTT, au niveau logique et physique, séparément des autres données. Cette recommandation a été acceptée par tous les organes impliqués lors d'une séance commune le 28 avril 1995. Les spécialistes de la sécurité informatique de l'OFI vont maintenant soumettre des propositions de cryptage alors que l'ODR, les PTT et l'OFI doivent élaborer, en collaboration avec une université suisse, un catalogue de mesures appropriées dans le cadre de l'évaluation des risques pendante à l'ODR. Sur cette base, l'ODR et les PTT élaboreront un règlement de traitement.

2.10. Système de décompte des coûts immobiliers et d'assistance LIFAS

Au cours d'une discussion survenue fin 1994 concernant l'avant-projet de ce nouveau système TED, nous avons, eu égard à la protection des données, rendu les organes compétents attentifs à la nécessité d'une gestion comptable aussi "indépendante que possible de la personne". Entre-temps, le Conseil fédéral s'est décidé pour le modèle d'une péréquation largement forfaitaire des coûts avec les cantons, ce qui non seulement facilite la gestion comptable, mais encore désamorce les problèmes de la protection des données. En outre, toute la partie assistance a été sortie du projet, de sorte qu'il n'y aura plus dans ce cadre de données sensibles relatives à la santé et à l'assistance. Le projet définitif nous sera présenté au moment voulu.

2.11. Révision de la loi sur le séjour et l'établissement des étrangers et de la loi sur l'asile

Dans le cadre de cette révision, le Conseil fédéral propose également aux Chambres fédérales l'adoption de dispositions relatives à la protection des données. Ainsi - comme le prévoit la LPD - seront fixés dans ces lois les traitements de données les plus importants, leurs buts et leur ampleur ainsi que la protection contre les traitements de données non autorisés. Par rapport aux projets du Conseil fédéral, les différences - elles sont au nombre de deux - concernent l'ampleur des accès online et l'étendue du traitement des empreintes digitales des personnes non criminelles.

Durant l'exercice écoulé, le Conseil fédéral a transmis aux Chambres fédérales sa décision de réviser la loi sur le séjour et l'établissement des étrangers et la loi sur l'asile. Les dispositions relatives au traitement et à la protection des données requises par la LPD figurent également dans les projets de révision. La collaboration entre l'administration et le PFPD peut être qualifiée de fructueuse. Comme nous l'avons mentionné dans nos premier et deuxième rapports d'activités (p. 110 ss, respectivement p. 118 ss), nous avons mis l'accent sur les revendications suivantes : une description détaillée des traitements de données sensibles, notamment au moyen de procédures d'appel ainsi que des buts du traitement; un examen minutieux des prescriptions de traitement des données sous l'angle de la proportionnalité/nécessité et de l'égalité devant la loi; une description suffisante des mesures protectrices spécifiques, notamment de la protection des tiers non concernés lors de traitements de données de police et du principe de la conservation séparée des données d'asile et de police; en outre, une description suffisante de la protection contre les transmissions non autorisées de données d'asile à l'étranger et dans le pays d'origine, notamment la description précise des transmissions autorisées (exceptionnellement) et de l'obligation de procéder dans chaque cas d'espèce à une pesée des intérêts *avant* la transmission; une limitation du traitement des empreintes digitales au strict nécessaire par le législateur.

Il est réjouissant de constater que ces travaux législatifs ont tenu compte, sous une forme ou une autre, de la plupart de ces requêtes importantes. Les différences résiduelles concernent les questions suivantes : le nombre d'autorités qui ont vraiment besoin d'un accès online aux fichiers centraux des données relatives aux étrangers et à l'asile pour l'exécution de leurs tâches, et la possibilité de leur transmettre d'une autre manière (de cas en cas ou par paquet et, le cas échéant, sous une forme anonyme) les données requises; la règle selon laquelle on prend en

principe les empreintes digitales de *tous* les requérants d'asile lors de l'entrée dans notre pays, de sorte que l'on ne peut pas ou pas suffisamment tenir compte de diverses circonstances; la durée de conservation des données enregistrées dans le système après la clôture d'une procédure d'asile ou de droit des étrangers. Nous attendons avec grand intérêt les décisions que le Parlement va prendre sur ces questions importantes.

Traités avec l'Allemagne et la Croatie
Un premier traité avec l'Allemagne, signé en 1995, porte sur *une comparaison unique de 3000 feuillets d'empreintes digitales de requérants d'asile* prises par les autorités allemandes en 1993 avec le fichier suisse AFIS d'empreintes traitées électroniquement. Au sens du traité, cette comparaison unique doit avoir lieu exclusivement dans un but statistique et devrait donner de plus amples informations sur la tendance présumée des requérants d'asile à demander l'asile dans plusieurs pays en même temps.
Dans notre prise de position, nous nous sommes limités uniquement à de pures considérations du droit de la protection des données, reprises intégralement dans le traité. Si l'on entre plus dans le détail, l'intérêt réside essentiellement en ceci : les données allemandes ne doivent pas être mémorisées dans l'AFIS; elles sont lues électroniquement par paquet dans une mémoire de travail et immédiatement effacées après la comparaison d'un paquet. Les éventuels "touchés", c'est-à-dire les empreintes concordantes, *ne* sont *pas* transmis aux autorités d'asile mais évalués anonymement. La comparaison est effectuée par les fonctionnaires de l'ODR spécialisés dans l'exploitation d'AFIS, et non par les fonctionnaires compétents en matière de procédure d'asile. Le PFPD surveille la comparaison qui doit lui être annoncée au préalable. Les feuillets d'empreintes digitales doivent être envoyés en Suisse de manière sûre et être retournés après comparaison à l'autorité allemande compétente (nous aurions aussi pu imaginer une destruction immédiate des copies sur papier après la comparaison en Suisse).

Finalement, le projet d'un accord sur le transit avec la Croatie nous a été soumis. Il correspond aux exigences formelles du droit de la protection des données. Nous avons rendu les autorités compétentes du DFJP attentives aux éventuels problèmes de transposition pratique et avons donné notre accord, à condition que nous soyons périodiquement informés, et que nous soyons associés dans les cas critiques. Simultanément, nous avons suggéré de compléter au sens de la LPD et du traité de transit la clause de reprise figurant dans l'accord de 1993 relatif aux visas.

3. Télécommunications

3.1. Internet - les garde-fous de l'autoroute de l'information sont encore bien mous

Même si certains utilisateurs présentent les premiers signes de désillusion, ne serait-ce qu'à cause des surcharges récentes du réseau, le développement fulgurant d'Internet a continué au cours de cet exercice. Grâce à une prise de conscience accrue des conséquences des activités du réseau et à des mesures appropriées, les risques toujours importants liés à la protection des données peuvent être limités.

Le réseau Internet est - comme tout le monde sait aujourd'hui - le plus grand réseau d'ordinateurs au monde. Il constitue cependant plus qu'une simple mise en réseau de réseaux individuels : Internet représente avec ses utilisateurs un espace de communication que l'on pourrait qualifier à juste titre de «global village», c'est-à-dire de village dans lequel les habitants s'envoient du courrier électronique et des fichiers entiers, discutent par l'intermédiaire de forums thématiques électroniques, mettent à disposition des informations de toutes sortes, offrent des produits et des prestations de service, font de la publicité pour leurs intérêts, etc.
L'Internet peut être considéré comme le premier niveau de réalisation, un peu comme l'aorte d'une «Global Information Infrastructure».

Les origines du réseau Internet actuel remontent aux années soixante, lorsque le Département de la défense des États-Unis mit sur pied un réseau conçu de manière à ce qu'il soit impossible de le mettre hors service par une destruction ponctuelle ciblée. Plus tard, ce réseau s'étendit aux universités, aux instituts de recherche et aux autorités. De plus en plus de participants se mirent à reconnaître l'utilité des possibilités de communication qu'offraient ce réseau, ce qui fait que de plus en plus d'institutions de différents pays se connectèrent au réseau. Un vrai engouement se fit sentir. Ce n'est qu'au début des années nonante que le grand public commença à remarquer Internet, lorsque de plus en plus de sociétés commencèrent à se connecter sur le réseau et que la possibilité fut offerte de participer à cette communication globale depuis sa maison à l'aide d'un ordinateur personnel.

L'Internet, en tant que moyen de communication interactif moderne, offre à ses utilisateurs, qu'ils soient fournisseurs ou consommateurs d'informations, d'énormes avantages. Il est ainsi possible de mettre à disposition rapidement et à peu de frais des informations toujours mises à jour qui peuvent être consultées à tout instant dans le monde entier à peu de frais. On y trouve des informations et des interlocuteurs dans tous les domaines d'intérêts possibles et imaginables; il n'existe pratiquement pas d'autre support permettant un tel libre échange d'opinions à l'échelle mondiale.

Comme nous l'avons mentionné plus haut, les utilisateurs de ce réseau mondial d'ordinateurs étaient jusqu'à il y a quelques années surtout des scientifiques et des collaborateurs d'administrations, d'universités et d'instituts de recherche. L'échange de données se faisait en quelque sorte parmi des initiés, au sein desquels régnait un rapport de confiance basé sur la collégialité.
Ces temps sont définitivement révolus. Suite à l'essor d'Internet qui a été déclenché par la diversité des offres et par des interfaces utilisateur graphiques très conviviales et constamment améliorées, le réseau est devenu attrayant pour un cercle d'utilisateurs bien plus large.
Les possibilités offertes aux utilisateurs d'Internet sont très variées et leurs motivations les plus diverses. Vu la diminution de la confiance réciproque qui régnait jadis parmi les utilisateurs, ainsi que d'une certaine autorégulation qui en découlait, les facettes sombres de notre société font également leur apparition sur le réseau. C'est cet aspect qui a procuré à Internet une célébrité plutôt douteuse dans les médias, parfois aussi suite à une exagération des faits.
Ont en particulier été l'objet de discussions des questions non résolues de droits d'auteur, la publication d'écrits interdits sous forme imprimée (par ex. du livre «Le Grand Secret» en France), la distribution de matériel pornographique sous forme de

textes, d'images et de sons, la diffusion de propagande politique incitant à la haine raciale, la publication de guides pour commettre des actes délictueux, etc.

Les systèmes juridiques actuels étant dans une large mesure limités aux territoires nationaux, les activités indésirables ne peuvent de nos jours plus être contrôlées de manière appropriée. Souvent l'utilisateur ne sait même pas dans quel pays les données qu'il consulte sont stockées.
Étant donné que l'utilisation du réseau implique également la communication de données personnelles qui sont transmises à grande échelle sous forme de contenu, ceci met en danger la protection des données pour les personnes concernées.

L'accès à Internet se fait par l'intermédiaire de prestataires de service, également appelés «provider». Alors que les doigts d'une main suffisaient récemment pour les compter, le marché suisse actuel compte plus de trente entreprises de tailles différentes et offrant des prestations très diverses. Entre-temps, les services de messagerie connus tels que Compuserve, America Online, Swiss Online (vidéotex) et d'autres se mettent à offrir à leurs clients un accès à Internet en plus de leur propre service.
Le prestataire de service a la possibilité technique d'analyser dans une large mesure le comportement de ses clients (au sujet desquels il connaît d'autres données grâce au lien commercial existant entre eux) en matière de communication. Il est en mesure de voir à quelles heures de la journée un utilisateur se connecte au réseau, quels sont les services qu'il utilise, quels sont les autres utilisateurs du réseau Internet avec lesquels il communique, et quelles informations il va chercher sur quels serveurs. Ceci lui permet de constituer des profils de la personnalité, ces assemblages de données qui permettent d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique. Le traitement de données personnelles n'est cependant autorisé que dans la mesure où il est nécessaire pour l'accomplissement des tâches du «provider» (facturation, etc.).
Le client devrait être informé des mesures techniques et organisationnelles prises par le prestataire afin qu'il puisse au mieux évaluer les risques qu'il encourt et adapter son comportement en conséquence.

L'utilisateur peut grandement améliorer la protection des données grâce aux mesures et aux comportements suivants (liste non exhaustive) :

- toute personne ayant l'intention d'injecter des données personnelles (propres ou relatives à des tiers) dans le réseau doit clairement savoir quelles en sont les conséquences. Souvent les questionnaires apparaissant sur le réseau Internet sont très complets et demandent de fournir des données sensibles. Nous recommandons de faire preuve de beaucoup de prudence et de retenue lorsque vous remplissez de tels questionnaires.
- Vu les énormes volumes de données accessibles sur Internet, le problème de la connectabilité des données est d'une grande actualité. Il est possible de regrouper des fichiers indépendants de données personnelles (par ex. des annuaires), de les dépouiller de manière systématique puis de les mémoriser, ce qui peut créer des risques impossibles à évaluer pour les personnes concernées. Les données accessibles publiquement sur Internet peuvent être analysées à l'aide de logiciels de recherche très sophistiqués et performants. Une fois que les données sont disponibles sur le réseau, la personne concernée n'est pratiquement plus en mesure d'en contrôler l'utilisation.

- Internet ne connaît pas de frontières nationales : il faut considérer que des données personnelles peuvent être transmises vers des pays qui ne disposent pas ou de très peu de dispositions de protection des données.
- De bons procédés de cryptage des données sont aujourd'hui disponibles et devraient être utilisés chaque fois que des données sensibles ou des profils de la personnalité sont transmis (par ex. par courrier électronique ou lors de transferts de fichiers). Il est également possible de vérifier l'intégrité des données transmises et l'authenticité de l'expéditeur grâce à des fonctions de signature numérique.
- Nombre d'entreprises, mais également d'administrations désirent profiter du potentiel d'information et de communication que leur offre Internet. C'est la raison pour laquelle ils ressentent le besoin de relier leurs propres réseaux d'entreprise à Internet. Afin de protéger les données internes contre un accès illicite en provenance de l'extérieur, toute communication entre les deux réseaux doit transiter par un ordinateur frontal intermédiaire (appelé «firewall»). Ce dernier est chargé de vérifier les droits d'accès. Une journalisation permet de détecter rapidement les attaques potentielles.

En Suisse, les participants au réseau Internet sont en outre tenus de respecter les dispositions de la LPD. Les mesures techniques et organisationnelles mentionnées dans l'ordonnance relative à la LPD doivent être appliquées.

Une utilisation commerciale à large échelle (commandes directes, transactions bancaires, etc.) sur Internet n'est pas pensable sans la présence de mécanismes de sécurité très poussés. Ces derniers servent également la protection des données. Il existe déjà plusieurs solutions pour certaines applications. Le prochain protocole «Internet Protocol Next Generation (IPng)» contiendra déjà des services de sécurité.

Il y a lieu au demeurant d'étudier si les personnes participant au processus de communication Internet seraient prêtes à accepter un code moral dans lequel elles s'engageraient à respecter des normes minimales de protection des données adaptées à leur domaine d'influence. Ces mesures ne doivent cependant en aucun cas représenter une censure du libre flux de données; il s'agit plutôt d'édicter certaines règles de trafic permettant d'éviter les utilisations abusives du réseau.

3.2. Révision de la loi sur les télécommunications

En vue de la suppression des derniers monopoles du secteur des télécommunications en Europe, une révision de la loi sur l'organisation des postes ainsi que de la loi sur les télécommunications à été engagée. Nous avons été appelés à prendre position à ce sujet dans le cadre de la consultation des offices.

D'ici 1998 au plus tard, les derniers monopoles des sociétés nationales de télécommunications d'Europe seront abolis. Afin que les Télécom PTT restent concurrentiels, leur monopole sera également supprimé. Il est prévu de soumettre le marché ainsi libéralisé à des conditions uniformes par une révision de la loi sur les télécommunications (LTC).

Nous avons eu l'occasion, dans le cadre de la première consultation des offices, de régler avec le service compétent quelques différends relatifs au projet de loi. Nous

avions défendu la position selon laquelle des dispositions relatives à l'utilisation des données concernant les télécommunications, l'identification du raccordement appelant ainsi que la sécurité des services de télécommunications contre une écoute et d'autres atteintes illicites devraient être introduites dans la loi. Cette exigence a été refusée motif pris qu'il s'agissait d'une loi du marché. Nous avons néanmoins réussi à nous mettre d'accord sur le fait que le Conseil fédéral sera tenu de par la loi de réglementer ces points en particulier.

Dans deux autres domaines nous n'avons malheureusement pas réussi à obtenir un accord.

Les PTT défendaient le point de vue selon lequel un enregistrement et une écoute des appels radio et des conversations téléphoniques était nécessaire pour des raisons d'assurance de qualité. Le fait que l'on enregistre à cette occasion le contenu des conversations enfreint largement le secret des télécommunications et constitue une atteinte à la personnalité. Nous sommes d'avis que les conditions préalables à de telles mesures doivent être mentionnées individuellement dans la loi. D'autre part, l'enregistrement et la surveillance du contenu des conversations n'est licite que si la loi définit une procédure d'autorisation. Cette procédure doit au minimum prévoir que la surveillance soit soumise pour approbation à une instance supérieure après une certaine durée. Elle doit également régler la durée de la mesure ainsi que la fréquence avec laquelle celle-ci est répétée.

En rapport avec les relevés de taxes détaillés, nous avons en outre défendu le point de vue selon lequel la réglementation actuelle de la LTC doit en principe être maintenue. Celle-ci prévoit que seuls les indicatifs des centraux locaux peuvent être communiqués, les dernières positions du numéro d'abonné appelé étant tronquées. Il est néanmoins nécessaire de prévoir des mesures dérogatoires pour l'obtention de preuves dans le cadre d'un procès en cours ou pour prouver l'intérêt d'un client digne d'être protégé.

3.3. La nouvelle loi sur le service des postes

La suppression du monopole des PTT dans le domaine des télécommunications modifie la position de la poste sur le marché. Afin de prendre en compte ces changements, l'actuelle loi sur le service des postes doit être révisée. Nous nous sommes prononcés à ce sujet dans le cadre de la première procédure de consultation des offices.

Selon les projets qui nous ont été remis, la poste bénéficierait d'une situation ambiguë. Ainsi, les secteurs d'activité de la Poste devraient être répartis en service universel et en service compétitif. Le service universel de son côté serait subdivisé en services réservés et services non réservés. Il est prévu que la Poste offre les prestations non réservées du service universel ainsi que les prestations compétitives en concurrence avec les prestataires privés. Les prestations réservées du service universel resteraient cependant monopole de la Poste. La Poste conserverait donc le droit exclusif d'acheminer les lettres affranchies ainsi que les paquets pesant jusqu'à 2 kilos. Quant aux paquets d'un poids supérieur, la Poste les acheminerait en concurrence avec les prestataires privés.

Le fait de distinguer entre service universel réservé et non réservé au niveau des envois postaux a pour conséquence que le traitement des données clients est soumis à des dispositions de protection des données distinctes. Pour le traitement des données des clients qui font acheminer des envois postaux jusqu'à un poids de 2 kilos par la Poste, les dispositions de la LPD relatives aux traitements de données personnelles effectués par les organes fédéraux sont invocables, alors que lorsqu'un client expédie un paquet d'un poids supérieur, ce sont les dispositions de la LPD applicables aux personnes privées.
Une différenciation au niveau des dispositions légales applicables en fonction du poids - le paquet pèse-t-il encore 2 kilos ou déjà 2,1 kilos ? - est à peine praticable. Étant donné que les rapports de droit entre la Poste et ses clients devront nouvellement être soumis au droit privé, on s'est mis d'accord pour que le traitement de données clients soit soumis aux dispositions de la LPD relatives au traitement de données personnelles par des personnes privées. La surveillance sera quant à elle régie par les dispositions applicables aux organes fédéraux.

Des divergences subsistaient eu égard aux exigences quant au contenu de la réglementation. Nous avions demandé à ce que soient ancrées dans la loi des dispositions concernant :
- la communication de données clients à des tiers;
- le droit des clients d'interdire la communication des données;
- le droit des clients d'interdire - après information préalable - le traitement de données qui ne sont pas nécessaires à l'exécution du contrat.

Comme dans le cas du projet de loi sur les télécommunications, on s'est mis d'accord pour que les détails ne soient pas réglés dans la loi mais dans des ordonnances du Conseil fédéral.

3.4. Base légale pour la mise à disposition par l'administration fédérale de données relatives à ses employés par procédure d'appel

De plus en plus d'employeurs se mettent à rendre accessibles, de manière électronique ou autre, des données concernant leurs employés. Un renforcement de cette tendance se fait également sentir au sein de l'administration fédérale.

Dans l'administration fédérale également, le désir des services de rendre accessibles des données concernant leurs collaborateurs, par ex. dans l'annuaire X.500 ou dans le WWW sur Internet - augmente.

La LPD exige une base légale expresse pour la mise à disposition de données personnelles par procédure d'appel, et même une base légale dans une loi au sens formel pour les données sensibles et les profils de la personnalité. Nous avons discuté cette exigence avec l'Office fédéral de l'informatique (OFI) dans le cadre du projet pilote X.500, ainsi qu'avec la Chancellerie fédérale qui désire rendre l'annuaire fédéral accessible par procédure d'appel. L'OFI a constitué un groupe de travail dont le but est d'élaborer une base légale suffisante. Ce groupe de travail comprend des représentants de la Chancellerie fédérale et de l'OFI ainsi que de nos services et est chargé d'élaborer une base légale valable pour l'ensemble de l'administration fédérale.

A cette occasion ont été soulevées les questions de savoir quelles données personnelles peuvent être rendues accessibles par procédure d'appel et à quelles fins. Les informations ont pour but de faciliter la communication avec les employés de l'Etat. C'est la raison pour laquelle nous sommes d'avis que seules les informations nécessaires à l'établissement de la communication avec le collaborateur concerné doivent être communiquées. Tout au plus pourrait-on ajouter d'autres données sur demande expresse du collaborateur concerné, pour autant que celles-ci soient restreintes aux informations qui sont en rapport direct avec l'exécution des tâches de ce dernier.

3.5. Communication d'adresses de cases postales au contrôle de l'habitant d'une ville par les PTT

Jusqu'à il y a peu de temps les PTT communiquaient au contrôle de l'habitant de la ville de Berne le nom et l'adresse des clients qui demandaient l'ouverture ou la restitution d'une case postale. La question de la licéité de cette communication s'est posée.

En recevant régulièrement les listes de mutation, le contrôle de l'habitant obtenait à notre connaissance également les adresses de cases postales des personnes résidant en ville mais qui ne s'étaient pas annoncées au contrôle de l'habitant, ainsi que les adresses des non-résidents.

La communication, par un organe fédéral, de données personnelles telles que les adresses de nouveaux détenteurs de cases postales ou les changements d'adresse nécessite une base légale. En vertu de l'ordonnance relative à la loi sur le Service des postes, les PTT peuvent communiquer sur demande aux expéditeurs les changements d'adresse de destinataires moyennant une taxe devant être fixée dans les dispositions d'exécution. Par conséquent, les changements d'adresses ne peuvent être communiqués à l'expéditeur d'un envoi postal que si le destinataire dispose déjà d'une adresse postale et que celle-ci a changé entre-temps.
Par le biais des listes de mutations, le contrôle de l'habitant recevait également les adresses des détenteurs de cases postales qui habitaient en dehors de la ville de Berne et n'étaient donc pas annoncés. Le contrôle de l'habitant ne disposait donc pas encore de l'adresse postale de ces personnes, ce qui signifie que la disposition correspondante de l'ordonnance relative à la loi sur le service des postes ne peut pas être prise comme base légale pour la communication de ces données.

La communication d'adresses de détenteurs de cases postales qui ne sont pas annoncés au contrôle de l'habitant est donc illicite.

3.6. Courrier électronique et annuaires électroniques

En 1995, le PFPD a eu l'occasion de tester un système de courrier électronique équipé de fonctions de sécurité et installé sur deux postes de travail, ainsi qu'un service d'annuaire de l'administration fédérale.

Le courrier électronique (E-Mail) est un moyen de communication souple et efficace qui est fréquemment utilisé de nos jours par de nombreuses entreprises et autorités. Normalement, ces systèmes sont rarement équipés de fonctions de sécurité, raison

pour laquelle on ne peut pas exclure que les messages transmis puissent être lus ou même manipulés par des personnes non autorisées. Il est en outre également possible de simuler de faux destinataires.
Un usage de plus en plus fréquent est fait des services d'annuaire qui permettent d'interroger les adresses télécom des partenaires potentiels de communication et parfois même d'autres données les concernant.

Lors d'une exploitation test pendant plusieurs mois d'un système de courrier électronique équipé d'un service d'annuaire de l'Office fédéral de l'informatique, le PFPD a pu se convaincre qu'il existe des produits permettant d'utiliser les fonctions de sécurité (basées sur des procédés de chiffrage) suivantes :
- confidentialité du message au cours de l'acheminement;
- intégrité du message, donc pas de modification non autorisée;
- possibilité de vérifier l'authenticité de l'auteur du message (signature numérique).

Comme nous avons pu le constater, les ordinateurs utilisés de nos jours dans le domaine de la bureautique sont assez performants pour permettre un cryptage/décryptage des messages électroniques sans provoquer pour autant de ralentissement notable du traitement. D'autre part, les applications sont faciles à manier.

Les fonctions de sécurité mentionnées ne peuvent être mises en oeuvre que si l'expéditeur *et* le destinataire disposent tous deux de l'équipement nécessaire et que la gestion des clés est clairement réglée (mot-clé : Trusted Third Party).

4. Personnel

Secteur privé

Conformément à l'article 328b CO, 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. (cf. sur ce thème également nos 1er et 2e rapports d'activités, p. 134 ss et p. 138 ss).

4.1. Tenue de listes des adresses privées des collaborateurs et collaboratrices

L'employeur ne peut tenir une liste des adresses privées des collaborateurs accessible à tous que si elle est indispensable aux activités professionnelles.

Un particulier s'est adressé à nos services pour savoir si l'employeur peut tenir une liste des adresses privées des collaborateurs et en permettre l'accès aux autres collaborateurs. L'employeur ne le peut que si la liste est nécessaire aux activités professionnelles, par exemple lorsque des employés doivent être régulièrement contactés à leur domicile. De même, l'employeur ne peut mettre cette liste à disposition des autres employés que si les activités professionnelles le requièrent véritablement. Mais lorsqu'il suffit que par exemple le central téléphonique puisse

atteindre les employés à leur domicile, l'employeur ne doit remettre cette liste qu'audit central. Lorsque les adresses privées des employés ne sont pas absolument nécessaires aux activités professionnelles, l'employeur n'est pas en droit d'établir de liste de ce type.

4.2. Contrôle des titres universitaires par l'employeur

Une université cantonale, l'Office fédéral de la santé publique et la Conférence suisse des recteurs peuvent et doivent réagir différemment à la requête d'un employeur désirant la vérification du diplôme d'un médecin employé chez lui, car ils sont soumis à différentes dispositions légales.

Une personne employant une femme médecin dans son entreprise désirait s'assurer que les données concernant son diplôme fournies par ce médecin au moment de l'embauche étaient justes. A cet effet, il contacte l'un après l'autre le centre de formation, à savoir une université cantonale, qui lui refuse le renseignement sans une déclaration de consentement signée de la main de la personne concernée, l'Office fédéral de la santé publique, qui ne voulut répondre à sa requête que sur demande écrite dûment motivée et enfin, la Conférence suisse des recteurs qui lui fournit volontiers le renseignement par téléphone. Dérouté par ces diverses réactions, l'employeur nous a demandé notre opinion.

Les diverses réactions à cette demande de renseignements s'expliquent par le fait que les différents services consultés sont soumis à des dispositions légales différentes. En tant qu'établissement cantonal d'enseignement, l'université est soumise à la loi cantonale sur la protection des données, alors que l'Office fédéral de la santé publique relève des dispositions de la loi sur la protection des données applicables aux organes fédéraux; enfin, la Conférence suisse des recteurs est soumise aux dispositions de la loi sur la protection des données concernant les personnes privées. La vérification de l'octroi ou du refus des renseignements par l'université n'était donc pas de notre compétence. En revanche, nous avons pu constater que la réaction de l'Office fédéral de la santé publique répondait aux dispositions correspondantes de l'ordonnance concernant les examens fédéraux des professions médicales et était donc correcte. Les informations à notre disposition ne nous ont en revanche pas permis d'apprécier la mesure dans laquelle la communication des données par la Conférence suisse des recteurs était licite. Dans le cas d'espèce, il aurait fallu contrôler que la communication des données ne se traduise pas par une atteinte à la personnalité de la personne concernée. Cela relève néanmoins du juge civil. Mais cette communication de données n'allait en tout cas pas fondamentalement à l'encontre des dispositions de la LPD relatives aux traitements de données par des personnes privées.

4.3. Communication de données concernant les salaires à des autorités fiscales étrangères

L'art. 328b CO ne s'oppose pas à la communication de données par une filiale en Suisse au siège principal à l'étranger lorsqu'elle est nécessaire à l'accomplissement d'obligations légales dudit siège selon le droit du pays concerné.

Les autorités fiscales belges avaient demandé à une société dont le siège principal était en Belgique et la filiale en Suisse des renseignements sur ses employés en Suisse. Elles demandaient notamment une liste des noms des frontaliers et le montant de leurs salaires, afin de pouvoir donner des renseignements aux administrations fiscales allemandes et françaises dans le cadre de l'examen de questions de double imposition.

Après avoir établi que selon la loi fédérale sur le droit international privé (DIP), les contrats de travail en question étaient soumis au droit suisse du travail, il a fallu examiner l'admissibilité de la communication des données à la lumière de l'article 328b CO. La communication de données à des autorités dans le cadre des obligations légales de l'employeur doit être considérée comme traitement de données nécessaire à l'exécution du contrat de travail. De ce fait, l'article 328b CO ne s'oppose pas à la communication de ce genre de données.

En revanche, la filiale en Suisse ne peut être obligée par les autorités belges à communiquer ces données. Seules les autorités suisses sont habilitées à le faire dans le cadre d'une demande d'entraide judiciaire.
(Cet avis de droit a été reproduit intégralement dans la JAAC 1995 II, p. 254 ss, avec ses considérants relatifs au DIP et au droit de double imposition.)

4.4. Droit d'accès des travailleurs - droit à la remise d'une expertise graphologique

Le travailleur a droit à la remise de la copie d'une expertise graphologique de son écriture, mais pas de l'original car celui-ci appartient à l'employeur. En cas de non-engagement et après la fin des rapports de travail, l'expertise graphologique doit être détruite.

Toute personne a le droit d'apprendre du maître d'un fichier quelles données la concernant y figurent. Les données doivent en général être communiquées par écrit, sous forme d'imprimé ou de photocopie. En accord avec le maître du fichier ou sur sa proposition, la personne concernée peut également consulter ces données sur place. Mais dans ce cas également, elle doit avoir la possibilité de demander des copies. Ce procédé peut être important notamment pour la consultation des dossiers du personnel. On ne peut restreindre le droit à obtenir une copie que dans le cadre de l'article 9 LPD, notamment en présence d'intérêts prépondérants de tiers ou de propres intérêts prépondérants. Les personnes concernées ont donc fondamentalement le droit d'obtenir une copie de l'expertise graphologique; en revanche l'employeur peut par exemple cacher le nom du graphologue.

Le travailleur a bien entendu le droit que lui soient remis les dossiers lui appartenant (dossiers de candidature à l'exception de la lettre de candidature, certificat d'assurance sociale, etc.). Par contre, lorsque les documents appartiennent à l'employeur, la remise de l'original ne constitue pas un droit. Une expertise graphologique étant en général commandée par l'employeur, donc lui "appartenant", le travailleur ne peut demander que l'original lui soit remis.

Le candidat qui n'est pas engagé a le droit de demander la destruction de tous les documents le concernant qui ne doivent pas lui être remis. Les expertises graphologiques en font partie. Durant le rapport de travail, l'expertise graphologique

peut être conservée comme pièce du dossier personnel, mais ne devrait pas être librement accessible à l'intérieur du dossier. Après achèvement du rapport travail, l'employeur n'est en droit de conserver que les données dont il a besoin pour la dissolution réglementaire du rapport de travail et pour l'accomplissement d'éventuelles obligations postcontractuelles (par ex. établissement du certificat ou comptabilité, obligations relevant du droit des assurances sociales). Toutes les autres données traitées doivent être détruites. C'est le cas des expertises graphologiques et des tests d'aptitude.

4.5. Surveillance des travailleurs - appareil de relevé électronique des compteurs

Un appareil de relevé électronique des compteurs peut également être utilisé pour le contrôle des prestations dans la mesure où il n'en résulte pas une surveillance systématique et générale des contrôleurs.

Il y a un certain temps, diverses centrales électriques ont introduit de nouveaux appareils de relevés des compteurs qui enregistrent le moment exact du relevé par l'employé. L'appareil permet aux collaborateurs autorisés de rechercher dans le système, lors du calcul de la consommation d'énergie, si le client le demande, quel compteur a été relevé à quelle date par quel employé. En même temps, il est possible d'évaluer la date et l'heure de chaque opération de relevé, à partir de quoi on peut voir à quel rythme l'employé en question a travaillé. Un employé d'une entreprise d'électricité s'est adressé à nous pour savoir si cela était conforme à la protection des données.

Nous avons demandé des précisions à l'entreprise qui nous a dit que le nouvel appareil n'était en principe pas utilisé pour surveiller les employés et que les données n'étaient pas interprétées en fonction d'une personne particulière. Lors de l'introduction de cet appareil, tous les employés chargés des relevés auraient été informés du nouvel appareil et du but de son utilisation. Ils auraient en outre reçu l'assurance qu'aucune donnée ne serait interprétée en fonction d'une personne particulière. A partir de février 1994, des contrôles par sondage auraient été effectués dans quelques cas en raison de problèmes concrets. Au cours d'une réunion en mai 1994, le personnel aurait été informé de ces contrôles. Par la suite, et dans un cas seulement, une évaluation aurait été effectuée durant quelques semaines encore.

L'employeur n'est en droit d'installer des systèmes de surveillance ou de contrôle que pour des raisons de sécurité ou pour calculer le rendement. Sont considérés comme systèmes de surveillance et de contrôle tous les dispositifs techniques qui permettent d'observer, séparément ou par groupes, les activités ou le comportement des employés. En font notamment partie les appareils décrits pour le relevé électronique des compteurs. Néanmoins, dans le cas présent, ces appareils sont utilisés avant tout pour faciliter la facturation. Les personnes concernées ont été informées des possibilités d'utilisation de l'appareil et l'utilisation prévue leur a été précisée. Il n'y a dès lors rien à objecter à l'utilisation de ce type d'appareil pour le relevé électronique des compteurs. Par contre, la surveillance systématique et permanente des employés à l'aide de cet appareil ne pourrait être autorisée, ne serait-ce que pour des raisons de protection de la santé, mais aussi du point de vue de la protection des données.

Administration fédérale

Le traitement de données du personnel par des organes fédéraux n'est pas seulement soumis aux dispositions de la LPD - plus restrictives que celles applicables au secteur privé - mais aussi à la loi sur le statut des fonctionnaires, y compris les dispositions d'exécution (circulaire de l'Office fédéral du personnel du 16 janvier 1984 concernant la protection des données relatives aux agents de la Confédération).

4.6. Remplacement de PERIBU par BVPLUS, et blocage des projets de gestion décentralisée des données du personnel

Depuis plusieurs années, il est question de remplacer PERIBU par un nouveau système, BVPLUS (cf. notre 1er rapport d'activités, p. 138 ss). Or, ce n'est qu'en janvier 1996 que les responsables de PERIBU nous ont informés de l'entrée en fonction prochaine de ce système, alors que ce dernier sera déjà testé auprès de quelques offices dès 1997.

Dans le cadre de l'examen du projet d'ordonnance du Conseil fédéral concernant la protection des données relatives aux agents de la Confédération, et de projets de traitement décentralisé des données du personnel, tels PIAS et PISEDI, nous avions notamment mis l'accent sur les points suivants (cf. notre 1er rapport d'activités p. 138 ss) :

- nécessité, respectivement obligation de collaborer avec le préposé fédéral dès le début de l'élaboration d'un projet, afin que les impératifs de la protection des données soient de suite pris en considération;
- coordination entre les responsables de PERIBU/BVPLUS et ceux des projets décentralisés;
- consultation du personnel et/ou de ses représentants.

Nous avons au demeurant encouragé, sous l'angle de la protection et de la sécurité des données, le développement de systèmes décentralisés de traitement de données du personnel, le système PERIBU/BVPLUS étant dès lors appelé à ne plus être qu'un système de gestion des salaires.
Au cours de nos quelques contacts avec le responsable de PERIBU/BVPLUS (notamment une séance en février 1992), nous avons souligné la nécessité de faire preuve de transparence et de nous tenir régulièrement au courant de l'évolution du dossier.

Or, ce n'est qu'en janvier 1996 que nous avons reçu une déclaration du fichier BVPLUS et de la documentation. Il ressort de cette dernière que le projet est suffisamment avancé pour être testé auprès de quelques offices dès l'an prochain. Nous avons également appris que les concepteurs de systèmes décentralisés avaient reçu l'ordre de bloquer de suite leurs travaux.

Fin janvier 1996, nous avons contacté l'organe responsable de BVPLUS afin de lui rappeler ses obligations légales, et de lui demander l'intégralité de la documentation relative au projet.

4.7. Etendue de l'obligation, pour un agent de la Confédération, de fournir des renseignements sur son état de santé aux fins d'admission au sein d'une caisse de pension

Notre médiation a été requise par une agente qui s'est vue infliger une réserve de la part de sa nouvelle caisse de pension. Cette dernière avait en effet prié la personne concernée de remplir un questionnaire ad hoc, et l'intéressée avait refusé de répondre à la question "avez-vous effectué un test-SIDA au résultat positif ?".

Nous avons tout d'abord constaté que la première partie du formulaire, concernant l'état de santé des parents et frères et soeurs de la personne concernée, n'était pas conforme à la LPD, vu qu'elle concernait des tiers. L'intéressée n'était au demeurant pas nécessairement en mesure de répondre correctement à ces questions.

Nous avons en outre souligné que la question relative au VIH était disproportionnée. En effet, les connaissances scientifiques en matière d'incidences de la séropositivité sur l'évolution de la santé sont insuffisantes pour justifier la focalisation sur le SIDA plutôt que sur d'autres maladies, telle la malaria. De ce fait, il n'est pas justifié d'infliger systématiquement une réserve de cinq ans aux personnes ayant répondu par l'affirmative à cette question, ainsi qu'à celles ayant refusé d'y répondre.

La caisse de pension a depuis lors annulé la réserve qu'elle avait émise à l'encontre de la personne concernée, et elle n'utilise plus le VIH comme critère de sélection. Le contenu du questionnaire soumis aux futurs membres de la caisse est actuellement en cours de révision.

4.8. Notion de données à usage exclusivement personnel

Une collaboratrice d'un office a requis notre médiation. Elle nous a signalé que son agenda avait été consulté par son supérieur, qui avait également photocopié des extraits de ce document. Ces copies avaient été transmises au service du personnel de l'office. L'intéressée avait également subi des pressions pour qu'elle détruise les pages photocopiées, ces dernières contenant des informations sur les allées et venues de certains collaborateurs, ainsi que des remarques les concernant.

Nous avons tout d'abord souligné que, du point de vue des règles générales de la protection de la personnalité, nul n'est habilité à consulter l'agenda d'une personne, et encore moins à en faire des photocopies, ni à exiger la destruction de certaines pages. Le détenteur dudit agenda est au demeurant libre d'y annoter ce que bon lui semble.

Il a en outre été indiqué que cet agenda ne constitue pas un fichier au sens de la LPD, du moment qu'il n'est pas structuré de manière à retrouver les informations par personne concernée. Nous avons également rappelé aux personnes impliquées dans cette affaire que ledit agenda n'est pas soumis à la LPD, vu qu'il contient des données qu'une personne physique traite pour un usage exclusivement personnel. Encore faut-il, pour qu'il y ait "usage exclusivement personnel", que les informations ne soient pas utilisées hors du cercle restreint de la vie privée et familiale, ce qui implique notamment qu'elles ne soient pas communiquées à des collègues de travail.

4.9. Questionnaire-annexe du certificat médical rempli par un candidat à un emploi

La personne concernée, suite à une absence prolongée pour maladie, a dans un premier temps été licenciée pour faute, pour avoir omis de mentionner, sur son questionnaire médical, des hospitalisations antérieures à son engagement. Sous l'angle de la protection des données, nous avons été appelés à nous prononcer sur la conformité du recours à un seul questionnaire, tant à des fins d'emploi que d'admission au sein de la Caisse fédérale d'assurance (CFA).

Nous aimerions tout d'abord souligner que le document qui nous a été soumis pour examen est une ancienne version, un nouveau formulaire ayant été établi dès 1989. Nos constatations ne sont donc susceptibles d'avoir des conséquences que pour les collaborateurs soumis à un examen médical effectué "sous l'ancien régime".

Après une absence prolongée de l'intéressée pour maladie, le département qui l'employait devait prendre une décision quant à la libération de son poste pour une autre personne, respectivement la mise en invalidité de la personne concernée. Or, le chef du personnel chargé de régler ce cas a été informé par le service médical que cette collaboratrice, lors de son engagement, avait omis de mentionner des hospitalisations antérieures, de crainte de ne pas être embauchée. Il a dès lors été décidé dans un premier temps de punir la personne concernée pour son mensonge, et de la licencier pour faute, ce qui aurait considérablement réduit les prestations sociales dues par la Caisse fédérale d'assurance.

Consultés par la mandataire de l'intéressée, nous avons constaté que l'ancienne pratique de la Confédération, qui consistait à utiliser un seul questionnaire médical pour deux finalités différentes (aptitude à l'emploi et admission dans la CFA) était contraire aux principes de proportionnalité et de finalité de la LPD. Le candidat à un emploi était en outre confronté à un dilemne : à l'égard de son futur employeur, le droit de mentir par nécessité est reconnu ("Notwehrrecht der Lüge"), alors qu'il ne l'est pas vis-à-vis de sa caisse de pension.

Quant au service médical, nous avons souligné que lorsqu'il est prié de fournir un rapport à un département, il n'est autorisé à communiquer par ce moyen que ses conclusions quant à la capacité, respectivement le degré et la durée d'incapacité de travail de la personne concernée. Le département décide, sur la base de ces conclusions, d'une éventuelle mise à l'invalidité de l'intéressé, respectivement de la remise de son poste au concours.
Nous avons finalement conclu que, dans un tel cas, *le département est tenu de rendre une décision objective*, n'étant pas autorisé à licencier un collaborateur pour faute, ni à informer, respectivement tenter d'informer la CFA des lacunes dont il a connaissance.

La CFA ayant déjà reçu les premières conclusions du chef du personnel du département lors de notre intervention, seule une partie de nos propositions a pu être suivie par ce dernier, par une objectivation de la formulation de la décision relative à la capacité de travail de la personne concernée.

4.10. Indication des motifs d'absence dans le programme hebdomadaire

La communication des motifs détaillés d'absence en cas de maladie (médecin, cure, maladie, convalescence, thérapie) dans un programme hebdomadaire qui n'est pas seulement accessible à l'entourage professionnel immédiat de la personne concernée, mais à un grand nombre de personnes, n'est pas conforme aux prescriptions de la protection des données.

La communication à des tiers des motifs d'absence du personnel en cas de maladie peut effectivement avoir pour conséquence une atteinte à la personnalité de la personne concernée. Conformément au principe de la proportionnalité, il n'est possible de traiter des données que dans la mesure et de la manière nécessaires pour atteindre le but fixé. En d'autres termes, les données sur la santé des agents ne peuvent être relevées par l'employeur que dans la mesure où elles sont nécessaires au déroulement du rapport de travail (notamment poursuite du versement du salaire et établissement du plan de travail pendant une absence pour cause de maladie). De même, ces données ne peuvent être communiquées par l'employeur à l'intérieur de l'administration qu'aux personnes qui en ont besoin du fait de leur activité (service du personnel, supérieurs et collaborateurs directs de la personne concernée). Pour les autres, il suffit en général d'une communication précisant que la personne concernée est absente durant une période déterminée.
Pour cette raison, il est conseillé de n'indiquer que l'absence dans le programme hebdomadaire, sans indication des motifs, tout en veillant à ce que le libellé choisi ne laisse pas entendre qu'il s'agit d'un problème de santé. Par exemple si dans tous les autres cas, le motif de l'absence est donné, l'absence de motif indique que celle-ci est due à la maladie. Il est donc recommandé de ne spécifier dans le programme hebdomadaire que les absences dues à un motif professionnel, et d'inscrire les absences pour d'autres motifs (maladie, vacances, congés, etc.) sous une dénomination unique.

4.11. Obligation faite aux employées du service des renseignements des Télécom PTT (no 111) de s'annoncer en mentionnant aussi leur prénom

Sans base légale appropriée, on ne peut obliger les téléopératrices du service des renseignements des Télécom à s'annoncer non seulement par leur nom mais également par leur prénom.

Une personne employée à la direction d'arrondissement de Genève désirait savoir si elle pouvait être obligée de s'annoncer avec ses nom et prénom lorsqu'elle décrochait pour fournir un renseignement. C'est ce qu'exigeait la direction d'arrondissement en invoquant une amélioration du service à la clientèle et la pratique dans le secteur privé. Les téléopératrices se sentaient atteintes dans leur sphère privée par cette obligation de dire leur prénom et craignaient d'être importunées par les clients. Un contrôle effectué auprès de la direction d'arrondissement de Genève (pour plus de détails, voir p. 170) a permis de conclure que l'indication du prénom n'avait aucune utilité concrète et qu'à diverses reprises, elle avait suscité des familiarités de la part des clients. Nous avons donc émis l'avis que sans base légale expresse à ce propos, on ne pouvait exiger des téléopératrices qu'elles mentionnent leur prénom. La direction d'arrondissement de Genève en informa ensuite ses employées.

4.12. Recommandations de l'Office fédéral du personnel sur l'application de méthodes de test individuelles et collectives

Suite à l'utilisation croissante de diverses méthodes de test individuelles et collectives en vue de la sélection du personnel au sein de l'administration fédérale, l'Office fédéral du personnel a élaboré des recommandations sur l'application de ces méthodes de test et nous les a soumises pour avis.

En effet, les méthodes de test individuelles ou collectives comme les expertises graphologiques, les tests psychologiques de performance, d'intelligence ou de personnalité, les questionnaires biographiques et autres systèmes d'évaluation (assessment, assessment center) jouissent d'une faveur toujours plus grande comme méthode d'évaluation des collaboratrices et collaborateurs actuels ou futurs. Dans notre deuxième rapport d'activités (p.142 ss), nous nous sommes déjà exprimés sur un test informatisé de la personnalité (Sigmund Potential) et avons indiqué les conditions d'une utilisation des données traitées conforme à la protection des données. Conformément à cet avis ainsi qu'au guide pour le traitement de données personnelles dans le secteur du travail par des personnes privées, l'Office fédéral du personnel a émis des recommandations sur la manière d'agir face à ces méthodes de test et nous les a soumises pour avis. Ces recommandations posent divers principes dont nous ne relèverons ci-dessous que ceux qui n'ont pas été déjà présentés dans le deuxième rapport d'activités.

- Si plusieurs personnes d'un même office fédéral ou d'une même entreprise fédérale participent à un test pour lequel l'anonymité ne peut être garantie, il faut les en informer au préalable.

- L'original des résultats du test doit être remis à la personne testée après achèvement de la procédure, et les autres documents (copies comprises) doivent être détruits.

- La personne testée doit dans tous les cas avoir la possibilité de se prononcer personnellement sur les résultats du test et leur interprétation.

- Les tests ne doivent pas être utilisés comme moyen unique ou principal; ils ne remplacent en aucun cas l'entretien personnel d'évaluation, de sélection ou de promotion.

- L'application de méthodes de test doit être précédée d'une analyse précise des performances requises; les résultats du test doivent donner des informations parlantes en rapport avec ces performances.

- Le nombre et le volume des divers tests et les résultats attendus doivent être adaptés au poste et coordonnés; l'engagement personnel, financier et en temps doit être apprécié avec un oeil critique en comparaison des résultats attendus.

- Les tests sont exclusivement du ressort de gens formés à cet effet.

- Il convient de garder une attitude critique vis-à-vis des résultats des tests.

- Les résultats isolés doivent être mis en rapport avec l'ensemble de la personnalité et des capacités de la personne testée.

- Il convient d'adopter une attitude correcte et transparente vis-à-vis de la personne testée; tous les résultats des tests doivent lui être présentés en lui donnnant la possibilité de prendre position.

- Il faut examiner quelles conceptions de l'être humain ou de la personnalité sont à la base de la méthode de test adoptée; celle-ci ne doit pas être choisie sans regard critique.

- Il convient d'examiner quelle méthode de test correspond le mieux à la "culture" de l'office ou de l'entreprise et à la fonction à examiner.

- L'interprétation des résultats du test est toujours subjective. Il convient de veiller à ce que l'on ne tente pas de légitimer cette subjectivité par l'objectivité apparente des résultats des tests; on devrait reconnaître qu'il s'agit d'une interprétation personnelle et le souligner à l'intention de la personne testée afin qu'elle puisse se prononcer à son sujet.

5. Assurances

Assurances sociales

5.1. Communication systématique du diagnostic aux assurances-maladie

L'entrée en vigueur de la nouvelle législation sur l'assurance-maladie remet d'actualité une question débattue depuis un certain nombre d'années par les partenaires concernés : celle de la communication systématique du diagnostic aux caisses-maladie. Nous avons été appelés à nous prononcer sur la légalité de cette communication.

La question du principe de la communication du diagnostic aux assurances-maladie, discutée depuis un certain nombre d'années par les partenaires concernés, est à nouveau d'actualité depuis l'entrée en vigueur de la nouvelle loi fédérale sur l'assurance-maladie (LAMal; voir également p. 158). Nous avons été appelés à nous prononcer sur la légalité de la communication systématique dudit diagnostic, telle que prévue dans le projet d'ordonnance sur l'assurance-maladie (OAMal).

L'article 42, 4e alinéa, LAMal prévoit que "l'assureur *peut exiger* un diagnostic précis ou des renseignements supplémentaires d'ordre médical", ce qui implique une demande de l'assureur effectuée dans un cas d'espèce. Or, le projet d'article 63, 1er alinéa, OAMal, dans sa version de janvier 1995, exigeait que les fournisseurs de prestations communiquent systématiquement ledit diagnostic. Nous avons d'une part constaté que ce mot aurait mérité d'être défini, afin de mettre un terme aux divergences d'interprétation y relatives. Nous avons d'autre part souligné que cette obligation de communication était illégale, car allant au-delà du cadre fixé par la LAMal, et contraire au principe de la proportionnalité. Nous avons finalement recommandé de prévoir, dans les cas où le recours au diagnostic est nécessaire,

l'utilisation d'une liste de codes-diagnostic cadres valable pour toute la Suisse, afin de mettre un terme aux disparités cantonales et d'assurer un niveau de protection des données équivalent à l'ensemble des personnes assurées en Suisse.

La nouvelle mouture du projet OAMal ne nous a pas été soumise une nouvelle fois pour avis, avant d'être adoptée par le Conseil fédéral le 27 juin 1995, puis d'entrer en vigueur le 1er janvier 1996. Nos propositions ont cependant été reprises pour la plupart dans un article 59 intitulé en ces termes :

[1]Les fournisseurs de prestations doivent indiquer dans leurs factures :
a. les dates de traitement;
b. les prestations fournies, détaillées comme le prévoit le tarif qui leur est applicable;
c. le diagnostic dans le cadre du 2e alinéa.

[2]Les assureurs et les fournisseurs de prestations peuvent stipuler dans les conventions tarifaires quelles informations et diagnostics ne doivent, en principe, être portés qu'à la connaissance du médecin-conseil de l'assureur au sens de l'article 57 de la loi. Au surplus, la communication du diagnostic est régie par l'article 42, 4e et 5e alinéas, de la loi. Le département peut fixer, sur proposition commune des assureurs et des fournisseurs de prestations, un code uniforme pour les diagnostics, valable dans toute la Suisse.

[3]Les prestations prises en charge par l'assurance obligatoire des soins doivent être clairement distinguées des autres prestations dans les factures."

La lettre c du premier alinéa de cette disposition doit être interprétée principalement à la lumière de la phrase du 2e alinéa mise en évidence en caractères gras. Or, la disposition de la LAMal qui y est évoquée est comprise de différentes manières, dont voici les plus courantes :

- la plupart des assureurs estiment que ces bases légales les autorisent à requérir des fournisseurs de prestations la communication systématique du diagnostic détaillé;

- Certains fournisseurs de prestations (dont ceux du canton de Genève, pour qui l'entrée en vigueur de ces nouvelles règles implique un changement radical de pratique en matière de facturation) estiment qu'en principe, la communication du diagnostic est exclue, cette dernière ne pouvant avoir lieu que sur demande et dans des cas d'espèce;

- un 3e courant, intermédiaire, considère que la loi, en prévoyant la remise au débiteur de la prestation de "*toutes les indications nécessaires* pour qu'il puisse vérifier le calcul de la rémunération et le caractère économique de la prestation", entend également la communication systématique d'un diagnostic. Celui-ci serait un diagnostic-cadre, dont le degré de précision reste à définir de manière conventionnelle par les partenaires concernés, par opposition au diagnostic détaillé. Ce dernier ne pourrait être fourni que dans des cas d'espèce et sur demande.

Nous nous sommes quant à nous ralliés à la deuxième "école", la plus conforme à la protection des données, après examen du message de la LAMal. Nous avons en outre conclu que l'OAMal ne peut être considérée comme conforme à la loi que dans ces limites. Il a finalement été constaté qu'il n'est pas établi, en l'état actuel des connaissances scientifiques en la matière, que le traitement systématique du diagnostic, si détaillé soit-il, soit un critère satisfaisant pour permettre la vérification des rémunérations et de l'économicité des prestations.

5.2. Liste des analyses et tarif

Lors de sa dernière séance, qui s'est déroulée le 31 mai 1995, le groupe de travail ADAK a adopté un projet de rapport intitulé Rapport du groupe de travail "Protection des données et liste des analyses / assurance-maladie" (ci-après rapport ADAK), contenant une synthèse des problèmes de protection des données se posant en particulier dans l'assurance-maladie, ainsi que des propositions de solutions (cf. également nos 1er et 2e rapports d'activités, p. 128 et p. 146). Les membres du groupe de travail ont insisté sur la nécessité de publier le rapport ADAK le plus rapidement possible, vu ses implications tant en droit des assurances sociales et privées, qu'en matière de droit du travail et de génie génétique. Ce document devrait également servir de base de réflexion à la Commission parlementaire travaillant sur le projet de loi fédérale sur la partie générale du droit des assurances sociales.
Or, nous devons malheureusement constater que le Département fédéral de l'intérieur n'a toujours pas diffusé le rapport ADAK.

5.3. Etendue de l'obligation des médecins de collaborer dans l'assurance-accidents

Un médecin a exprimé ses doutes quant à la compatibilité de la convention liant les assureurs-accidents et la FMH avec la LPD. Certaines clauses prévoient en effet la remise systématique de copies de rapports médicaux aux assurances.

Nous avons tout d'abord souligné que même si la législation sur l'assurance-accidents contient des normes qui obligent les médecins à communiquer les informations requises par les assureurs, il n'en demeure pas moins que ces communications doivent avoir lieu dans les limites de la LPD, en particulier de principes généraux tel celui de la proportionnalité. Ceci implique qu'un assureur n'est habilité à demander, puis traiter, que les données médicales nécessaires au règlement des sinistres. Or, vu que les clauses conventionnelles de communication que nous avons examinées ne respectent pas ce principe, nous avons conclu à leur illicéité.

Assurances privées

5.4. Feuille d'information et clause de consentement

Suite à nos remarques relatives au caractère lacunaire des feuilles d'information ("Merkblatt"), respectivement des clauses de consentement ("Einwilligungsklausel"; cf. notre 2e rapport d'activités p. 148), de nouvelles propositions de formulation de ces documents nous ont été soumises par des assureurs pour avis. Nous avons

rappelé à cette occasion la nécessité de faire preuve de transparence et avons proposé des clauses de consentement différenciées, en prenant l'exemple de l'assurance-vie.

La collaboration aux fins d'améliorer le libellé des feuilles d'information et des clauses de consentement se poursuit, tant avec des assureurs de personnes que de choses. Dans ce contexte, ces derniers nous ont soumis de nouvelles propositions de formulation. Nous avons relevé une amélioration de la transparence de la feuille d'information, sous réserve de certains compléments à apporter principalement aux rubriques concernant le consentement (révocable en tout temps) et le droit d'accès.

Pour ce qui est de la clause de consentement, nous avons également constaté que la formulation était plus précise, notamment quant aux tiers susceptibles d'être consultés et aux finalités des échanges de données prévus. Nous avons en revanche rappelé qu'une seule clause générale standard n'est pas suffisante pour que le consentement de l'intéressé puisse être considéré comme valable et couvrir non seulement les traitements de données en relation avec la conclusion d'un contrat d'assurance, mais encore tous les développements à venir dudit contrat, sans oublier le marketing. Une telle clause, avons-nous souligné, peut être considérée comme nulle de plein droit.

Nous avons dès lors recommandé d'établir une distinction entre les *clauses nécessaires*, à savoir dont la signature par la personne concernée est nécessaire à l'assureur pour établir et développer une relation contractuelle, et les *clauses subsidiaires*. L'assureur aimerait voir signer ces dernières, par exemple afin d'être habilité à utiliser des données à des fins de marketing. Dans ce cas, ledit assureur n'est pas autorisé à faire dépendre la conclusion d'un contrat d'assurance de la signature d'une telle clause.

Proposition a ensuite été faite de distinguer entre les *relations précontractuelles* et *contractuelles*, et d'adopter des clauses propres à chaque branche d'assurance. Une assurance de choses (pour immeubles par exemple) ne nécessite pas, pour sa gestion, la même masse de données personnelles qu'une assurance de personnes. De même, au sein de cette catégorie, la fréquence et l'intensité des flux d'informations ne sont pas les mêmes pour une assurance-vie que pour une assurance-maladie. Nous avons pris l'exemple de l'assurance-vie et proposé les solutions suivantes :

- au stade précontractuel, adoption d'une clause de consentement nécessaire, dont la durée de vie peut être limitée à la fin de la relation précontractuelle. Ceci implique, dans les cas où aucun contrat n'est conclu, la destruction des données relatives à l'intéressé, sous réserve de quelques exceptions (obligations légales de conserver des données, mauvais payeurs notoires, cas relevant du droit pénal etc.). Dans de tels cas, une durée de conservation des données limitée entre cinq et dix ans selon les motifs est envisageable.
  Si la personne concernée signe à ce moment-là une clause subsidiaire spécifique au marketing, l'assureur pourra conserver les données nécessaires à cette fin;

- au stade contractuel, une clause de consentement ne sera pas nécessaire, si les données sont traitées dans les limites des principes généraux de la LPD,

respectivement de ce que requiert la gestion d'un contrat d'assurance-vie (traitement objectivement fonctionnel).
Le consentement de l'assuré sera en revanche demandé chaque fois qu'un événement spécifique, comme la survenance d'un sinistre, appellera des traitements de données débordant le cadre habituel décrit au paragraphe précédent. En cas d'incapacité ou de décès de l'assuré, le consentement de son représentant légal sera demandé;

- quant au cross-selling, utilisé en marketing, il fera le cas échéant l'objet d'une clause subsidiaire spécifique. Il faut en effet que la personne concernée ait la possibilité de s'y opposer sans que ce refus ait d'incidences sur le contrat d'assurance lui-même.

Le fait que les assureurs, de leur côté, signent également une clause par laquelle ils s'engagent à respecter le devoir de discrétion et les modalités de traitement de données décrites dans la feuille d'information a finalement été salué. Nous avons demandé de compléter cette clause par les rubriques suivantes :

- promesse, dans les cas où aucun contrat n'est conclu, de détruire les données devenues ainsi inutiles (avec les réserves susmentionnées);

- en cas de conclusion du contrat, garantie de l'information de l'intéressé et de l'octroi d'un délai approprié, lorsque des données provenant d'un tiers sont susceptibles d'avoir des conséquences négatives pour la personne concernée. Cette dernière pourra ainsi faire valoir le cas échéant son droit d'être entendu;

- promesse de demander le consentement de l'assuré, respectivement de son représentant légal, dans les cas d'espèce où les traitements de données dépassent le cadre de la LPD (en cas de sinistre par exemple).

5.5. Assurance pour véhicules automobiles

Suite à la déréglementation, respectivement libéralisation de la concurrence entrée récemment en vigueur dans ce secteur, les assureurs tentent d'obtenir de nombreuses informations des personnes concernées, afin notamment d'adapter au mieux leurs produits au marché. Dans ce contexte, un particulier nous a soumis un formulaire de proposition pour examen sous l'angle de la protection des données.

Nous avons tout d'abord rappelé que l'ensemble des activités des assureurs est régi par la LPD et ses principes généraux, dont celui de la proportionnalité. Nous avons au demeurant signalé que l'entrée en vigueur de la LPD a également pour conséquence de réduire la portée de la norme générale de déclaration obligatoire à charge du proposant, telle que prévue dans la loi fédérale sur le contrat d'assurance. L'importance d'une question ne peut plus être présumée du seul fait qu'elle figure dans le formulaire de proposition (Antragsformular). Encore faut-il, du point de vue de la protection des données, que la réponse à cette question ne soit pas seulement *confortable*, mais également *nécessaire* à l'assureur pour décider de l'issue de la proposition.

Nous avons constaté que le contenu du formulaire de proposition ne répond que partiellement aux critères susmentionnés, l'étendue des questions n'étant pas toujours en relation directe avec la conclusion du contrat d'assurance.

Quant à la clause par laquelle l'intéressé doit consentir à la communication de données personnelles le concernant à des tiers, nous avons finalement considéré qu'elle est illégale, vu son caractère beaucoup trop général.

Des discussions sont actuellement en cours, afin de trouver une solution à la fois praticable et conforme aux exigences de la protection des données.

6. Santé

6.1. La Commission d'experts du secret professionnel en matière de recherche médicale

Cette commission, qui existe depuis le 27 janvier 1994, autorise dans certaines conditions bien précises l'utilisation de données personnelles pour des projets de recherche médicale. Jusqu'ici il aurait été nécessaire pour tous les projets de recherche médicale utilisant des données personnelles d'obtenir le consentement de toutes les personnes concernées. Dans un grand nombre de cas, cette démarche était si peu praticable que bon nombre de projets de recherche médicale portaient en fait atteinte au secret médical et étaient donc illégaux. La mise sur pied d'une commission d'experts en mesure d'octroyer de telles autorisations reflète la tentative du législateur de mettre fin à cette situation intenable.

La commission se base sur l'article 321bis du code pénal suisse (CP) entré en vigueur le 1er juillet 1993 en même temps que la LPD. Elle se compose de onze membres au total nommés par le Conseil fédéral, qui représentent de manière paritaire les groupes intéressés (chercheurs, patients, médecins). Elle comprend donc trois représentants du domaine de la recherche, trois médecins praticiens et trois représentants d'organisations de défense des droits des patients. Il est en outre impératif que deux des membres soient juristes. Le secrétariat de la commission est assuré par l'Office fédéral de la santé publique, où une collaboratrice juridique est chargée de cette tâche à plein temps. Mis à part son rattachement administratif au Département fédéral de l'intérieur, cette commission est indépendante.

Sur les 29 demandes d'autorisation acceptées comme telles - avant tout pour des registres médicaux et des projets de recherche particuliers - la commission en a autorisé 21 et rejeté deux (il n'y a eu qu'un seul cas dans lequel le rejet de la demande a débouché sur la non réalisation du projet de recherche. Dans l'autre cas, une autorisation n'était pas nécessaire, du moment que le projet ne violait pas le secret médical). Six demandes sont encore pendantes.

Pour les projets de recherche qui ne peuvent pas être conduits avec des données anonymes et pour lesquels il est impossible ou très difficile d'obtenir le consentement des personnes concernées, la commission peut autoriser la levée du secret médical dans les cas suivants : d'une part on autorise des médecins praticiens à mettre à disposition des données de patients pour un projet de recherche précis. D'autre part on permet aux chercheurs de demander des données de patients

auprès des médecins praticiens, sans générer pour autant d'obligation de communiquer les données pour les médecins traitants.
La commission évalue au demeurant si les intérêts de la recherche priment ceux liés au maintien du secret.

La commission d'experts octroie d'une part des *autorisations particulières* pour des projets de recherche bien définis, le traitement des mêmes données dans le cadre d'un autre projet nécessitant une nouvelle autorisation séparée. D'autre part, elle dispense des *autorisations générales* à des organes gérant des registres médicaux (autorisations de registre) ainsi qu'à des cliniques qui conduisent régulièrement des projets de recherche (autorisations de clinique). La commission assortit ces autorisations de charges destinées à assurer la protection des données. Il s'agit de consignes concernant la conservation des données sensibles, la gestion des autorisations d'accès et, le cas échéant, la destruction des dossiers papier et des supports de données. Le PFPD est chargé de veiller au respect de ces charges. A l'occasion du démarrage de cette activité dans le domaine du registre épidémiologique des tumeurs, il s'est avéré que, "l'activité de surveillance" prescrite par la loi mise à part, les chercheurs responsables désiraient une certaine aide pour l'interprétation des décisions d'autorisations.

Pour compléter, mentionnons encore les trois autres tâches prévues par la LPD dans le domaine de la recherche médicale : tout d'abord il s'agit de conseiller la commission d'experts, ensuite le PFPD est tenu de faire le nécessaire pour que les patients soient informés de leurs droits, et finalement il peut contester les décisions prises en faisant recours auprès de la Commission fédérale de la protection des données.

6.2. Application de la LPD aux hôpitaux cantonaux

Lors de traitements des données de patients par les hôpitaux cantonaux, il faut de temps en temps vérifier si une relation médecin-patients est régie par le droit privé ou public et si l'on a affaire au droit fédéral ou cantonal. Selon la jurisprudence du Tribunal fédéral, l'assistance apportée aux malades dans les hôpitaux publics par des médecins dans l'exercice de leur fonction publique n'est pas considérée comme une activité économique de la collectivité.

Un particulier nous a demandé si la LPD ou la loi cantonale sur la protection des données était applicable aux hôpitaux publics du canton de Zurich. La loi sur la protection des données du canton de Zurich ne s'applique pas lorsqu'un organe est soumis aux principes de la concurrence économique et que dans ce cadre, il n'agit pas au nom de sa souveraineté (paragraphe 3, lettre a de la loi sur la protection des données du canton de Zurich). Dans ce contexte, différents rapports médecin-patients ont été examinés, notamment pour savoir si les hôpitaux de droit public agissaient à titre souverain.

Lorsqu'un patient est traité par son médecin dans un hôpital (de droit public) sur la base d'une relation contractuelle de droit privé, cette activité est régie par le droit des obligations. Le médecin est ainsi considéré dans ce domaine comme une personne privée et les dispositions de droit privé de la LPD s'appliquent.

La protection des données dans les hôpitaux cantonaux est une tâche incombant à l'organisation administrative cantonale, d'où l'obligation pour les cantons d'édicter des règles fixant le traitement des données personnelles au sein de l'administration publique cantonale et communale. La loi sur la protection des données de chaque canton concerné s'applique donc aux hôpitaux de droit public. La question s'est posée pour le canton de Zurich de savoir si les hôpitaux de droit public agissaient à titre souverain. Selon la jurisprudence du Tribunal fédéral, les soins aux patients dans les hôpitaux publics ainsi que ceux prodigués par les médecins dans l'exercice de leur fonction publique sont fournis à titre souverain et ne doivent pas être considérés comme une activité économique de la communauté (ATF 102 II 47 et 101 II 183, confirmés dans ATF 115 Ib 179 E. 2). Par conséquent, les hôpitaux de droit public agissent souverainement et ne participent pas à la concurrence économique. Ceci implique l'application de la loi cantonale sur la protection des données.

6.3. Droits d'accès et de consultation des patients

Le droit d'accès est un élément fondamental du droit de la protection des données et permet en principe à chaque patient de consulter les données relatives à sa santé et à son anamnèse (histoire médicale). Dans certains cas d'exception, d'autres personnes (tiers) peuvent aussi consulter le dossier d'un patient.

En principe, le droit d'accès doit être exercé par la personne concernée elle-même (droit strictement personnel) et personne ne peut y renoncer. Lorsqu'un patient n'est pas en mesure de faire valoir son droit d'accès, pour des raisons physiques ou psychiques, ses représentants légaux (par exemple les parents ou un tuteur) peuvent agir à sa place. Le droit d'accès peut être exercé indépendamment d'une procédure (par exemple procès civil ou pénal).

Si un tiers (par exemple un proche) veut prendre connaissance du dossier, le patient doit au préalable délier le médecin de son secret médical et donner son autorisation pour la communication correspondante. C'est seulement ensuite que le dossier peut être présenté à un tiers. Les parents ou d'autres représentants légaux n'ont aucun droit de consultation si un enfant mineur mais capable de discernement a été en consultation médicale et qu'il ne veut pas accorder à ses parents l'autorisation de prendre connaissance du diagnostic.

Le droit de consultation joue un rôle prépondérant dans des procès et procédures en cours car les parties ou leurs représentants ont le droit de consulter les dossiers. Pour l'acceptation d'un intérêt public ou privé supérieur au droit de consultation, il faut des éléments essentiels tangibles. Dans chaque cas, il faut procéder à "une pesée minutieuse et complète des intérêts en présence conformément à l'appréciation légale et dans le respect du principe de la proportionnalité" (ATF 115 V 301f). En d'autres termes, il faut dans tous les cas tenir compte des circonstances et intérêts particuliers.

Un tiers peut aussi exiger d'avoir connaissance, sans l'accord de la personne concernée, des données relatives à la santé de personnes décédées dans la mesure où

- le requérant prouve un intérêt à la consultation et

- sa demande n'est pas contraire aux intérêts prépondérants de proches de la personne décédée ou de tiers (proche parenté ou mariage; article 1er, 7e alinéa, OLPD).

En principe, lorsqu'un patient décède, son dossier ne peut pas être sans autre rendu accessible à des tiers. Il faut qu'il y ait eu une relation étroite entre la personne décédée et celle qui demande la consultation, et en plus que le demandeur justifie d'un intérêt réel à la consultation (sans intérêts contraires de tiers). Si ces conditions sont respectées, rien ne s'oppose à une autorisation de consulter.

6.4. Contrôles de communication, de mémoire et d'utlisation dans le domaine médical

Afin que la protection des données puisse être appliquée efficacement dans la pratique médicale, certaines mesures techniques déterminées sont impératives. Les contrôles de communication, de mémoire et d'utilisation en font partie. Toutefois, les meilleures mesures techniques ne sont valables que si elles sont aussi appliquées par les utilisateurs.

Contrôle de communication

L'expéditeur de données relatives à la santé doit garantir que ces dernières parviennent exclusivement au destinataire ayant droit. Dans tous les cas, on doit pouvoir reconstituer après coup qui a communiqué quoi, à qui et dans quel but. On peut ainsi par exemple éviter qu'un laboratoire d'analyses fasse parvenir les résultats d'un test du sida à un destinataire non autorisé.

Lors de la transmission de données par fax, on ne peut pas exclure que le document parvienne à un autre destinataire que souhaité. L'expéditeur endosse la responsabilité de la transmission, raison pour laquelle il a intérêt à ce que les informations ne tombent pas en des mains étrangères. Pour des données sensibles, il est recommandé d'avertir au préalable le destinataire afin de garantir un accès conforme à la protection des données. La transmission devrait être chiffrée et l'appareil de fax préparé de sorte que seules les personnes autorisées puissent avoir connaissance des documents reçus. Au cas où un message fax est remis par erreur à un faux destinataire, ce dernier devrait en informer l'expéditeur. On pourrait par exemple faire figurer sur le fax la clause supplémentaire suivante : "Si vous n'êtes pas le destinataire de l'adresse, veuillez s.v.p. avertir immédiatement l'expéditeur par téléphone et détruire ensuite le fax."

Contrôle de mémoire

Afin que les données relatives à la santé ne puissent être modifiées ou effacées illicitement, les utilisateurs doivent prouver leur légitimité par une attestation d'utilisateur (User-ID) et un mot de passe. En outre, pour protéger ces données contre la perte, il est impératif d'effectuer régulièrement des copies de sauvegarde et de les conserver dans un coffre. Il faut de plus empêcher que ces données puissent être copiées illicitement sur un support de données, par exemple sur une disquette. A cette fin, les lecteurs de disquettes peuvent par exemple être bloqués.

Les documents écrits sont un moyen de preuve important (par exemple lors de contestations en matière de droit de la responsabilité civile), étant donné que les modifications, suppressions et compléments ultérieurs sont très souvent reconnaissables. En ce qui concerne les enregistrements électroniques, il en va tout autrement : dans la plupart des techniques d'enregistrement, un effacement, un rajout ou une correction ultérieurs dans le système remplacent, sans laisser de traces, ce qui a été précédemment mémorisé. Afin d'augmenter la force probante des documents électroniques, il faudrait utiliser des systèmes qui excluent toute modification de données et de textes saisis et qui mentionnent comme tels dans un document les compléments ultérieurs. L'indication automatique de la date de chaque nouvelle introduction accroît également la sécurité contre les falsifications.

Contrôle d'utilisation

Il faut empêcher que des personnes non autorisées aient accès à des données relatives à la santé par le biais d'équipements de communication de données. Les systèmes informatiques doivent donc être conçus de manière à ne pas compromettre la confidentialité et l'intégrité des données par l'installation d'une maintenance à distance ou par des réseaux accessibles au public.

6.5. Le secret médical lors de l'évaluation de la charge de travail dans les hôpitaux et établissements médico-sociaux du canton de Vaud

Avec cette étude, le canton de Vaud désire répartir les subventions qu'il accorde aux hôpitaux et établissements médico-sociaux du canton de manière aussi équitable que possible. Cette étude est faite en collaboration avec les établissements mentionnés selon une méthode développée au Québec. Nous avons été approchés par les responsables de cette enquête nous demandant de clarifier les questions relatives à la protection des données qui se posent lors de la communication des données au service de coordination du projet à Lausanne ainsi qu'à la centrale de saisie des données à Montréal.

Pour chacun des établissements participant à l'étude, le déroulement de l'enquête peut être décrit ainsi :

- le personnel soignant de l'établissement remplit un questionnaire pour chaque pensionnaire. Parmi les informations fournies se trouvent également des données sensibles qui concernent la santé physique et mentale du pensionnaire.
- Par l'intermédiaire du service de coordination de Lausanne, les questionnaires sont transmis au Québec pour saisie et contrôle. Lors de la saisie et dans le traitement qui suit, on vérifie pour chaque questionnaire s'il est complet, ainsi que certains critères de plausibilité.
- Afin de pouvoir corriger les erreurs et compléter les indications manquantes, les contrôleurs du Québec doivent contacter un membre du personnel soignant de l'établissement concerné connaissant bien le pensionnaire auquel le questionnaire se rapporte.

Le moyen le plus simple, qui consiste à demander les précisions en mentionnant le nom du pensionnaire, constituerait cependant une atteinte au secret professionnel. Il fallait donc trouver un moyen permettant d'une part aux contrôleurs du Québec de demander des précisions dans l'établissement concerné au sujet de certains pensionnaires, et garantissant d'autre part qu'un lien entre certaines personnes et

leurs maladies ou traitements médicaux ne puisse être établi qu'au sein de l'établissement. Nous présentons ci-dessous la solution trouvée qui répond aux deux exigences formulées :

- le home établit une liste dans laquelle il attribue un numéro à chaque personne (liste des pensionnaires).
- Avant que le questionnaire quitte l'établissement, les noms sont rendus méconnaissables et remplacés par le numéro correspondant.
- Les personnes qui traitent les données au Québec contactent en cas de questions l'établissement concerné et demandent les informations relatives à un pensionnaire en mentionnant le numéro figurant sur le questionnaire de ce dernier.

6.6. La disposition particulière relative au droit d'accès aux données médicales - interprétation

L'article 8, 3e alinéa, LPD stipule que le maître du fichier *peut* faire communiquer des données concernant la santé d'une personne concernée par l'entremise d'un médecin désigné par cette dernière. Nous tenons à éclaircir ci-dessous brièvement le sens de cette disposition souvent mal comprise ainsi que l'interprétation qui en découle.

Le droit d'accès constitue un élément central de la protection des données parce que personne n'est en mesure de demander que les données le concernant soient corrigées ou détruites tant qu'il ne sait pas quelles sont les données que le maître de fichiers traite à son sujet. C'est pour cette raison que le droit d'accès est réglé de manière assez détaillée autant dans la LPD que dans l'OLPD, prévoyant en principe un droit à des renseignements fournis par écrit et gratuitement. La disposition particulière de l'article 8, 3e alinéa, LPD est libellée comme suit : "Le maître du fichier peut communiquer à la personne concernée des données sur sa santé par l'intermédiaire d'un médecin qu'elle a désigné."

Cette exception au droit d'accès direct écrit a un champ d'application très restreint. Il s'agit des cas dans lesquels la personne qui demande le renseignement pourrait recevoir un éclaircissement dommageable découlant d'un renseignement fourni directement et sans préparation. Le fait que cette disposition doit être appliquée de manière restrictive ressort de la tendance, de nos jours dépassée, de mise sous tutelle qui y apparaît de manière sous-jacente. Le fait que le législateur ait opté pour la formule *peut* plutôt que *doit* est également en faveur d'une interprétation restrictive. On ne peut par contre pas déduire de la formule *peut* que le maître du fichier a le droit de transmettre le renseignement par l'intermédiaire d'un médecin. Le maître de fichiers doit plutôt proposer ce moyen lorsque l'octroi direct du droit d'accès risque selon toute vraisemblance de générer un dommage grave. Dans tous les autres cas, les renseignements doivent être fournis à la personne concernée directement et par écrit.

6.7. Remise d'un certificat médical aux héritiers d'une personne décédée

Le droit d'accès selon l'article 8 LPD ne s'applique qu'à la personne concernée. L'article 1er, 7e alinéa, OLPD règle la consultation des données de personnes décédées et ne constitue pas au sens strict un cas d'application du droit d'accès. Nous avons répondu par l'affirmative à la question de savoir si l'on peut remettre à

l'épouse d'une personne décédée une copie du certificat de décès établi par l'hôpital traitant.

Dans le cas concret, une compagnie d'assurance avait refusé de remettre à la veuve une copie du certificat médical que l'hôpital avait établi sur le décès de son mari. Elle justifiait ce refus en argumentant qu'il lui était interdit de transmettre à des tiers des documents médicaux sans procuration du médecin traitant. La demande adressée par la veuve à l'Office fédéral des assurances sociales nous a été transmise par ce dernier en nous priant de bien vouloir prendre position du point de vue de la protection des données.

Nous sommes arrivés à la conclusion qu'il pouvait être donné suite à la demande de la veuve. Il est vrai que selon l'article 8 LPD le droit d'accès est réservé exclusivement à la personne concernée et n'est pas transmissible, ni à des personnes vivantes ni par testament. Mis à part les cas, dans lesquels la personne concernée est incapable de discernement et où les parents peuvent par exemple faire valoir le droit d'accès en qualité de représentant légal de leur enfant, le droit d'accès ne revient même pas à la parenté. Ces derniers peuvent uniquement faire valoir leur propre droit d'accès, pour autant qu'il existe. L'article 1er, 7e alinéa, OLPD, octroie en principe un droit de consultation aux proches parents de personnes décédées, droit qui est cependant limité par d'éventuels intérêts prépondérants de proches de la personne décédée ou de tiers. Dans de tels cas, le médecin peut être considéré comme tiers, raison pour laquelle on ne peut pas exclure a priori que le droit de consultation puisse être limité par les intérêts prépondérants de ce dernier. La tentative d'éviter d'éventuelles demandes de dommages-intérêts ne peut cependant pas justifier un tel intérêt.
Il convient d'autre part, lors de la pesée des intérêts, de prendre en considération la protection de la vie privée de la personne décédée. Ainsi le Tribunal fédéral a confirmé par une décision du 26 avril 1995 que la consultation du dossier médical d'une personne décédée ne peut être autorisée au fils de cette dernière que par l'intermédiaire d'un médecin. Il justifia sa décision en relevant en particulier que cette procédure permettait d'une part au fils d'obtenir les renseignements requis dans la mesure où cela se justifiait, d'autre part de préserver la confidentialité des données médicales. On peut entre autres en conclure que même lorsque de proches parents font valoir un intérêt au sens de l'article 1er, 7e alinéa, OLPD, il y a lieu de procéder à un examen approfondi des intérêts en présence en tenant également compte du but poursuivi par la demande de renseignements. Dans le cas présent - contrairement à la décision mentionnée du Tribunal fédéral - la demande se limitait à l'obtention d'une copie d'un seul certificat médical et non à consulter le dossier médical en entier. C'est pourquoi la pesée des intérêts ne doit pas être faite de manière aussi poussée, et rien ne s'oppose à ce qu'il soit donné suite sans autre à la demande de consultation qui nous a été soumise pour avis.

6.8. Développement du système MediData

La société MediData SA s'est fixé pour but de promouvoir l'échange électronique de données entre tous les partenaires du marché suisse de la santé. Elle propose de remplacer les flux de factures imprimées et de garanties de prise en charge par des messages UN/EDIFACT et de rationaliser ainsi le déroulement des affaires. Du point de vue de la protection des données, il faut relever comme point négatif le fait que les partenaires se recrutent parmi les assureurs et les fournisseurs de prestations, mais

n'englobent pas les assurés eux-mêmes. Comme point positif de ce système en cours d'élaboration, relevons que le problème de la confidentialité des données lors de leur transmission a été pris en compte.

La norme UN/EDIFACT permet un échange électronique de messages normalisés. Ce procédé, déjà largement utilisé entre autres dans le commerce international, permet de rationaliser les tâches de routine. L'objectif de MediData SA, dont les actionnaires principaux sont des compagnies d'assurance, est d'obtenir également de tels effets de rationalisation dans le «marché de la santé». Une économie de temps et de coûts n'est cependant possible que si des messages à structure similaire peuvent être échangés avec une certaine fréquence. C'est la raison pour laquelle cet échange électronique de messages n'est prévu qu'entre assureurs et fournisseurs de prestations. C'est surtout pour les messages contenant des données médicales sur le patient que nous déplorons que la personne concernée ne fasse pas partie du circuit.
En ce qui concerne le système actuellement mis en route, le PFPD prévoit de surveiller trois points en particulier :

- du point de vue de la protection des données, la question majeure qui se pose à propos de cet échange électronique prévu de messages est de savoir quelle est la masse de données médicales qui accompagneront chaque facture transmise de manière électronique du fournisseur de prestations à l'assurance. Il est clair et cela est également prévu dans la Loi fédérale sur l'assurance-maladie (LAMal) que certaines données indispensables au contrôle de routine des factures doivent toujours être transmises. Il est cependant aussi clair que des diagnostics précis ne peuvent être communiqués à l'assureur que dans des cas d'espèce si celui-ci en fait la demande (cf. également p. 146).
- Il faut à tout prix éviter de saper le droit des assurés prévu dans la LAMal qui leur permet d'exiger que des informations d'ordre médical ne soient communiquées qu'au médecin-conseil de l'assurance.
- Vu que la majorité des utilisateurs sont des organes fédéraux, il s'agira d'examiner si ces derniers disposent des bases légales leur permettant de recourir à un produit tel que MediData.

7. Crédit

7.1. Traitement de donnés lors de demandes de cartes de crédit

Celui qui présente une demande de carte de crédit accepte que les indications qu'il fournit soient vérifiées et transmises à certains organes déterminés. La transmission de ces informations à d'autres tiers sans information préalable de celui qui fait la demande ne repose sur aucun motif justificatif.

Un particulier s'est adressé au Préposé fédéral à la protection des données pour demander des éclaircissements en raison d'une indication inexacte figurant sur la nouvelle carte de crédit qui lui avait été remise. Suite à cette intervention, le déroulement de la procédure de demande, la formule de demande et les conditions générales de l'entreprise de cartes de crédit concernée ont été soumis à un examen plus approfondi.

Avec la demande de carte de crédit, l'entreprise de cartes de crédit obtient les indications suivantes sur le client : nom, prénom, adresse, date de naissance, nationalité, état civil, profession, situation professionnelle, revenu, relations bancaires, utilisation d'autres cartes de crédit, modalités de paiement et signature du requérant. Pour une demande de carte supplémentaire, on exige le nom, le prénom, la date de naissance et le lieu d'origine de la deuxième personne.
Le requérant confirme par sa signature l'exactitude des données indiquées et autorise l'entreprise de cartes de crédit à les vérifier à n'importe quel moment. Simultanément, il accepte les conditions générales, l'entreprise de cartes de crédit lui garantissant quant à elle le traitement confidentiel de toutes les données.

Les données sont prélevées pour vérifier les indications personnelles et la solvabilité du requérant ainsi que pour assurer la gestion ultérieure. L'exactitude des données personnelles est vérifiée à l'aide de l'annuaire de téléphone électronique. Si le requérant n'y figure pas, des recherches sont effectuées auprès du contrôle de l'habitant de sa commune de domicile. La solvabilité du requérant est vérifiée auprès de l'Association pour la gestion d'une centrale d'information de crédit (ZEK). En cas de relations financières particulièrement peu sûres, on consulte de surcroît l'Association suisse des émetteurs de cartes (KARTAC), laquelle gère en Suisse les informations relatives à la solvabilité du client en Suisse. En fonction de la situation, des recherches complémentaires sont effectuées auprès du contrôle de l'habitant, des offices de poursuites et faillites ou des autorités fiscales. Avant de procéder à des investigations auprès d'autres tiers, une discussion a lieu avec le requérant.

L'entreprise de cartes de crédit concernée est membre de la KARTAC, elle-même affiliée à la ZEK. Elle fournit à la KARTAC des informations relatives à la personne concernée telles que poursuites, motifs des blocages de cartes (par exemple faillite privée), moralité et capacité de paiement; ces informations peuvent être utilisées par d'autres membres.
En acceptant les conditions générales, le requérant autorise l'entreprise de cartes de crédit *"à rechercher tous les renseignements nécessaires à l'évaluation de la commande de carte. Cela signifie qu'il autorise la transmission des données dans la mesure qui découle des documents contractuels ou des documents généralement accessibles au cours de l'exécution du contrat; il donne également son accord pour la communication desdites données à des tiers déterminés par l'entreprise de cartes de crédit (par exemple organes centraux) et dont l'intervention est nécessaire à l'évaluation des risques et à l'exécution du contrat*. *Les organes centralisés peuvent expressément rendre ces données accessibles à d'autres membres des différents organismes centraux. Cette autorisation vaut également pour les contrôles correspondants effectués dans le cas d'autres demandes de cartes de crédit et pour les commandes futures".* Par ces indications, le client est vaguement informé de la transmission de ses données, mais il ne sait pas qui se trouve derrière les organismes centralisés, ni qui en sont les membres et quelles données sont communiquées.

Une atteinte à la personnalité n'est pas contraire au droit si elle est justifiée par le consentement du lésé (personne concernée). Afin que la personne concernée puisse donner son accord à bon escient, elle doit toutefois être informée de manière circonstanciée du traitement de ses données personnelles ainsi que du but poursuivi. Celui qui signe une demande de carte de crédit donne tacitement son accord pour le traitement de ses données personnelles par le partenaire contractuel,

de même que pour l'enregistrement et l'utilisation ultérieure, mais pas pour la transmission à des tiers qui ne sont pas clairement désignés. Comme le client donne son accord pour le traitement et la vérification, les données le concernant ne devraient pas être transmises à des tiers non définis pour des buts non déterminés et ainsi être utilisées ultérieurement par d'autres entreprises. C'est la raison pour laquelle le motif justificatif du consentement n'est en l'espèce pas donné.
La vérification et le traitement des demandes de cartes de crédit par l'entreprise de cartes de crédit elle-même ont lieu en relation directe avec l'exécution d'un contrat. C'est pourquoi il existe réellement un intérêt prépondérant et le traitement interne des données personnelles est justifié.

Compte tenu du grand nombre de demandes de cartes de crédit (opérations de masse) qui sont quotidiennement examinées par les différentes entreprises de crédit, une quote-part d'erreurs minimale (donnée inexacte sur une carte de crédit nouvellement émise) ne peut pas être exclue.
Comme le traitement des données personnelles effectivement entrepris ne ressort ni de manière exhaustive ni clairement de la demande ou des conditions générales, il en découle pour le requérant que le but, ainsi que les destinataires précis de ses données personnelles et leur traitement ultérieur ne sont pas reconnaissables. Cela signifie que le requérant ne sait pas de manière suffisante à quoi il consent (pas de droit suffisant à l'autodétermination de l'usage de ses données) et qu'il ne peut de la sorte pas s'opposer à un traitement de ses données. C'est pourquoi il est nécessaire d'apporter des précisions à la demande et aux conditions générales. Chaque requérant doit pouvoir reconnaître à qui ses données personnelles sont remises pour examen et pour quelles autres démarches il donne son accord. Avant que le client débute une relation contractuelle, il faut lui donner l'occasion de s'informer de manière circonstanciée sur les points suivants (par exemple sur une feuille d'information ou dans les conditions générales) :

- qui est le maître du fichier ?
- Quel est le but du traitement de données ?
- Auprès de quels organes/autorités les données sont-elles vérifiées ?
- uelles données sont transmises, à qui et dans quels buts (pour les personnes morales, il faut indiquer les destinataires ou membres avec plus de précision) ?
- omment s'effectuent la transmission (online ou sur papier) et la conservation ?

L'entreprise de cartes de crédit a finalement été priée de réviser les formules de demande de cartes de crédit et/ou les conditions générales en conséquence.

7.2. Octroi du droit d'accès en cas de refus d'une demande de carte de crédit

Bien qu'il soit mentionné dans les conditions générales d'une entreprise de cartes de crédit qu'aucune correspondance ne sera échangée en cas de refus d'une demande de carte, le droit d'acccès doit être garanti. Un passage dans la formule de demande de carte de crédit ou dans les conditions générales, excluant toute information n'est pas valable.

Une entreprise de cartes de crédit doit en principe communiquer gratuitement à la personne qui le demande toutes les données la concernant contenues dans le fichier. En outre, il faut indiquer le but du traitement et les catégories de données

personnelles traitées, les participants au fichier ainsi que les destinataires des données. L'information écrite ou la décision motivée sur la restriction du droit d'accès doit être donnée dans les trente jours dès réception de la demande. Sinon, le maître du fichier doit indiquer au requérant dans quel délai les informations lui seront remises. Les renseignements ne peuvent être refusés, limités ou différés que si une loi au sens formel le prévoit ou s'il y a nécessité en raison d'intérêts prépondérants d'un tiers ou du maître du fichier et que les données personnelles ne sont pas communiquées à des tiers. Au cas où le maître du fichier refuse, restreint ou diffère l'octroi du droit d'accès, il doit en indiquer la raison. Une mention dans la demande de carte de crédit ou dans les conditions générales qui exclut le droit d'accès n'est pas valable étant donné que le droit d'accès est un droit strictement personnel et que l'on ne peut pas y renoncer.
En cas de refus du droit d'accès, la personne concernée a la possibilité de déposer contre l'entreprise de cartes de crédit une plainte pour violation de la protection de la personnalité. Les plaintes pour non-respect du droit d'accès peuvent être déposées au domicile du plaignant ou du défendeur.

7.3. Créanciers sans protection à cause de la protection des données ?

Un créancier qui a reçu de son débiteur un acte de défaut de biens dont les indications lui paraissent douteuses doit s'adresser à l'office des poursuites et faillites compétent et non pas aux autorités fiscales ou à l'employeur.

Un créancier avait reçu un acte de défaut de biens dont le contenu lui paraissait douteux. Sur ce, il a voulu vérifier auprès des autorités fiscales et chez l'employeur si les indications correspondaient effectivement à la réalité. Les autorités fiscales et l'employeur s'appuyèrent sur la loi sur la protection des données et ne fournirent aucune information. Le créancier s'est senti lésé dans ses droits en tant que citoyen libre et s'adressa à nos services.
Les actes de défaut de biens sont des pièces officielles (du droit des poursuites pour dettes et faillites) qui ont toute leur validité tant que l'on n'a pas prouvé leur inexactitude. L'exactitude des indications figurant sur un acte de défaut de biens doit être vérifiée par le préposé de l'office des poursuites concerné ou l'autorité de surveillance dudit office. Ni les autorités fiscales, ni l'employeur ne peuvent donner à un créancier des renseignements sur l'exactitude ou l'inexactitude des indications figurant sur un acte de défaut de biens. Du fait qu'ils sont soumis à des règles particulièrement sévères, les registres des poursuites pour dettes et faillites sont exclus du champ d'application de la LPD.

Par conséquent, on ne peut pas dire que les créanciers sont lésés en raison des dispositions relatives à la loi sur la protection des données.

8. Marketing direct

8.1. Généralités

Régulièrement des personnes nous communiquent que malgré le blocage de leur adresse à des fins publicitaires et même des injonctions expresses dans ce sens

auprès d'une entreprise précise, elles reçoivent encore ses envois publicitaires. Nous recherchons depuis longtemps les moyens d'éviter ce genre de cas.

Nous avons déjà posé le problème dans notre premier rapport d'activités (p.148). Nous avions alors établi que la difficulté de garder une vue d'ensemble sur le traitement des données et par conséquent l'impossibilité de le contrôler posent un problème particulier. Il est en effet souvent impossible de déterminer l'origine d'un traitement d'adresse; en outre, les possibilités de blocage des adresses (PTT et liste Robinson) ne suffisent pas à juguler la distribution non désirée d'envois publicitaires. Depuis, nous avons régulièrement reçu des réclamations de personnes qui, malgré le blocage de leur adresse et après de multiples interdictions expresses, continuaient à recevoir les envois publicitaires d'une firme précise.
Au printemps 1995, nous avons procédé à un sondage auprès des associations des professionnels de la branche. Le questionnaire comportait une partie générale destinée aux associations faîtières qui abordait les questions du manque de transparence, du blocage effectif des adresses, de l'atteinte aux principes généraux de traitement des données (en particulier au principe de finalité) et enfin le problème particulier de la publicité par téléphone et par fax. Des solutions étaient proposées pour chaque type de problème et les associations faîtières étaient priées de prendre position. Dans ce même questionnaire, une partie spéciale était destinée aux firmes qui pratiquent le marketing direct; on y demandait des données sur le secteur d'activités, les données personnelles traitées, le mode de traitement, les droits de la personne concernée et l'organisation interne (responsabilité du traitement des données, mesures de sécurité prises, etc.). Cette rubrique pouvait aussi être remplie de manière anonyme.

Nous n'avons malheureusement reçu que peu de réponses à notre questionnaire. Plusieurs organisations faîtières sous l'égide de la Publicité Suisse (PS) nous ont demandé un entretien et leurs membres ont suspendu jusque-là la réponse à notre enquête. L'Association suisse pour le Marketing direct, l'Association suisse de Vente par Correspondance et la Publicité Suisse étaient présentes à cet entretien qui a eu lieu le 18 octobre 1995. Ils estimaient que la profession possédait déjà un haut degré d'autorégulation grâce à divers codes d'honneur et qu'elle ne se sentait pas tenue d'agir particulièrement dans le domaine de la protection des données.

Du fait du manque de soutien de la part des organisations faîtières, nous n'avons pas reçu les informations dont nous avions un besoin urgent sur le traitement des données pratiqué par les entreprises de marketing direct. Nous avons donc décidé de procéder au cours de cette année à des contrôles auprès de plusieurs firmes de marketing direct actives dans différents domaines. Notre intention est de nous faire une idée des traitements de données sur place pour établir sur la base des renseignements rassemblés une analyse de chaque problème du point de vue de la protection des données.

8.2. Transmission d'astérisques à des recueils privés d'abonnés

Les personnes qui ne désirent pas recevoir de publicité peuvent bloquer leur adresse ou leur numéro de fax auprès des PTT. Elles figurent alors dans l'annuaire téléphonique avec un astérisque (*). Les PTT sont autorisés à transmettre ces adresses pour l'établissement d'annuaires d'abonnés privés. Certaines adresses

bloquées ne sont toutefois pas reprises comme telles, ce qui se traduit pour les personnes concernées par la réception de nombreux envois publicitaires.

Nous avons reçu dès l'année dernière plusieurs questions à ce sujet. Par exemple un professionnel du traitement d'adresses se renseignait pour savoir à quelles conditions il était en droit d'utiliser à des fins commerciales les adresses figurant dans les annuaires téléphoniques, régionaux ou électroniques. Par ailleurs, diverses personnes se sont plaintes de recevoir des envois ou des appels publicitaires malgré le blocage de leur adresse ou de leur numéro de fax. Enfin, un préposé cantonal à la protection des données a attiré notre attention sur le fait que divers annuaires électroniques sur supports de données ne reprenaient pas les blocages.

L'ordonnance sur les services de télécommunications prévoit que les données des abonnés qui ne désirent pas recevoir de publicité peuvent être transmises uniquement pour la constitution d'annuaires d'abonnés privés. Les PTT se doivent de fixer les conditions de cette transmission et à cet égard de veiller au respect des prescriptions sur la protection des données. La vente d'adresses de clients des PTT à des tiers est réglementée dans une directive de service. Celle-ci prévoit que la transmission de données dans le but d'établir des annuaires d'abonnés privés est possible même si le client ne souhaite pas recevoir de publicité et a bloqué son adresse. Sont bloquées pour la vente les adresses des abonnés au téléphone et au téléfax qui ont interdit que leur adresse soit transmise. Ces adresses sont néanmoins remises pour l'établissement d'annuaires téléphoniques privés locaux et de CD-ROM. L'astérisque apparaît dans les annuaires imprimés avant le numéro d'appel et dans les versions sur écran à partir de CD-ROM, on peut lire la mention "ne désire pas de publicité" (les possibilités de blocage existent aujourd'hui pour les annuaires des services de téléphone et de téléfax, mais pas pour les recueils de vidéotex et de télex). Un libellé similaire figure dans les conditions de livraison d'adresses provenant des annuaires des Télécom PTT. Il y est néanmoins précisé que le traitement de ces adresses pour des mailings directs n'est pas autorisé. Si l'acheteur contrevient à ces conditions de livraison, les Télécom PTT peuvent immédiatement suspendre la livraison de données, si nécessaire de manière définitive.

La Direction générale des PTT nous a confirmé que les PTT rappelleraient ses obligations au producteur d'annuaires d'abonnés qui commettrait l'erreur de ne pas transmettre plus loin le blocage à des fins publicitaires, et suspendraient la livraison d'adresses en cas d'infractions réitérées. Nous avons contacté divers producteurs de supports de données qui reproduisent l'annuaire téléphonique électronique; selon eux, les blocages n'avaient pas été repris à l'origine (souvent en raison de difficultés techniques), mais avaient été rajoutés par la suite.

9. Statistique

9.1. Recensement 2000

Les préparatifs du recensement 2000 battent leur plein. Les travaux en vue de l'introduction d'une autre méthode de relevés se concentrent actuellement sur les problèmes de faisabilité technique et sur les conditions-cadres juridiques qui autoriseraient un recensement de la population à partir de registres cantonaux et

communaux (relevé indirect). Entre-temps, la Commission de gestion du Conseil national a chargé le Conseil fédéral d'étudier de nouvelles solutions aux méthodes de relevé du recensement.

Dans notre deuxième rapport d'activités (p. 135), nous avons présenté les conditions-cadres dans lesquelles la méthode de relevé du recensement peut être modifiée en vertu du droit de la protection des données.
Un recensement sur la base de registres (relevé indirect) est préférable à divers égards à un relevé à partir de questionnaires (relevé direct). Les raisons principales sont les suivantes :

- les communes, les cantons et la Confédération accomplissent leurs tâches à un moindre coût;
- l'efficacité et l'exactitude des données du recensement peuvent être accrues à moindres frais (rationalisation des relevés);
- le recensement est mieux accepté par la population car cette méthode est moins pesante pour les personnes recensées.

Dans ce sens, la Commission de gestion du Conseil national a chargé le Conseil fédéral d'examiner deux aspects :

La simplification du recensement 2000
Dans le cadre des possibilités actuelles, il faut appliquer une méthode de relevé plus simple et meilleure marché. Dans cette même optique, il convient également d'examiner la question de l'harmonisation, à des fins statistiques, des registres de technique administrative de la Confédération, des cantons et des communes. En outre, il convient aussi de contrôler les mesures de promotion de la collaboration entre Confédération, cantons et communes en matière d'harmonisation des registres régionaux de données.

La nouvelle orientation du recensement 2010
Pour que les données du recensement puissent être relevées au moyen de registres (relevé indirect), le Conseil fédéral doit créer les bases légales et constitutionnelles nécessaires, permettant également l'harmonisation des registres des cantons et des communes.

Ainsi que nous l'avons déjà mentionné dans notre deuxième rapport d'activités, une révision des méthodes de relevé des données du recensement est à juger de manière tout à fait positive. Dans ce contexte, le principe de finalité de la loi sur la protection des données et de la loi sur les statistiques doit être respecté. Cela signifie que les données personnelles ne doivent être utilisées que dans le but pour lequel elles ont été collectées à l'origine. La loi sur le recensement fédéral de la population exclut même tout utilisation non statistique des données du recensement.

Nous demeurons d'avis que les données collectées à des fins statistiques (données du recensement) ne doivent pas être utilisées simultanément ou ultérieurement à des fins administratives. Même les données d'un relevé fait à partir de registres doivent uniquement être utilisées à des fins statistiques. La loi sur la statistique fédérale prévoit certes une disposition permettant l'utilisation à d'autres fins de données personnelles relevées à l'origine à des fins statistiques. Mais elle ne concerne que des cas d'espèce et nécessite une base légale formelle.

Contrairement à la loi suisse sur la statistique fédérale, la législation européenne (Union Européenne et Conseil de l'Europe) interdit toute utilisation non statistique de données personnelles collectées à l'origine à des fins statistiques.

9.2. Constitution de systèmes de traitement des données au niveau national

La constitution de systèmes centraux traitant à des fins statistiques des données personnelles concernant l'ensemble de la population suisse peut devenir problématique du point de vue de la protection des données.

Les tâches de la statistique officielle sont aujourd'hui de première importance, notamment parce que grâce aux informations statistiques, le public est informé, les établissements planifient leur politique d'entreprise, l'Etat prend ses décisions et définit ses objectifs. Pour obtenir des valeurs statistiques valables pour toute la Suisse, il faut saisir et traiter des données personnelles concernant l'ensemble de la population. Le traitement d'une grande quantité de données est plus efficace lorsque les données sont gérées à partir d'un registre central.
Les données personnelles nécessaires aux statistiques sont relevées soit directement auprès de la population ou indirectement par le biais des registres des administrations cantonales et fédérales. Il est possible de mettre sur pied des fichiers dits auxiliaires afin de gérer ou d'exploiter les données collectées et de réduire les relevés périodiques longs et coûteux. Ces fichiers auxiliaires contiennent des codes ("Merkmale") ou des données qui permettent d'interconnecter divers autres fichiers. Dans certains cas, ces renseignements sont des données personnelles (adresse, domicile, etc.) ou peuvent permettent d'identifier des personnes. Du point de vue de la protection des données, ces fichiers ne sont pas problématiques s'ils servent exclusivement des buts statistiques (combiner des résultats, faciliter des relevés).

Récemment encore, il était difficile d'établir des registres centraux (que ce soit dans un but administratif ou statistique) du fait de la structure fédéraliste de la Suisse. Les cantons tiennent leurs propres registres en fonction de leurs besoins, et parallèlement les autorités fédérales compétentes disposent de registres traitant des données au niveau national. L'établissement de registres centraux nationaux est considérée comme la meilleure option et de ce fait encouragée afin de rendre la coordination entre les tâches fédérales et cantonales plus efficace, et surtout réduire les coûts de traitement des données. Indépendamment des problèmes juridiques existants qui entravent la constitution et l'établissement commun de registres centraux, le traitement central des données offre, sous l'angle de la protection des données, aussi bien des avantages que des inconvénients.

La gestion de systèmes centraux de traitement des données présente des avantages surtout parce qu'ils permettent une augmentation de l'efficacité et une réduction des coûts. Dans certaines circonstances, le risque d'atteinte à la personnalité s'en trouve néanmoins accru. Du point de vue organisationnel, le traitement central des données accroît le danger que les données soient traitées de manière illégale. S'ajoute à cela le fait que les personnes concernées perdent simplement la vue d'ensemble des innombrables traitements de données effectués sur la base de leurs données. De ce point de vue, de petits systèmes locaux offrent une meilleure vue d'ensemble et sont exposés à des dangers moindres.

Nous ne sommes pas opposés à la création de systèmes centraux de traitement des données. Nous partageons en principe l'avis d'autres autorités cantonales et fédérales selon lequel il est nécessaire de mettre sur pied un traitement central des données efficace et économique. Mais pour le citoyen, ce traitement doit offrir une bonne vue d'ensemble et être transparent. En d'autres termes, chaque citoyen doit savoir en tout temps par quelles autorités et à quelles fins ses données sont traitées. Les données personnelles ou les fichiers qui sont relevés ou constitués exclusivement à des fins statistiques ne doivent pas être utilisés à des fins administratives. La question de l'efficacité et des coûts ne doit pas servir d'argument pour un détournement de finalité.

Nous suivrons attentivement l'évolution de cette question, car le passé a montré que les registres centraux établis à l'origine à des fins statistiques sont utilisés peu d'années plus tard à des fins administratives et de contrôle.

9.3. Critères d'anonymisation des données personnelles ?

Au cours de l'exercice écoulé, nous avons été priés à plusieurs reprises de nous exprimer sur la notion de données anonymes. On suppose manifestement qu'il existe une règle générale applicable à tous les cas où des données personnelles sont rendues anonymes. On ne peut néanmoins définir de manière exhaustive les éléments qui permettent d'identifier une personne. C'est pourquoi il convient de définir dans chaque cas d'espèce les critères d'anonymisation des données personnelles.

Les données personnelles sont réputées anonymes lorsqu'on en a retiré les données permettant l'identification de la personne concernée. Si le rapport de certaines données à une personne particulière disparaît, ces données perdent leur caractère personnel. Les éléments d'identification à éliminer pour empêcher que l'on puisse reconnaître la personne concernée changent de cas en cas. Souvent il suffit d'effacer le nom et l'adresse. Mais lorsque des renseignements de nature particulière permettent l'identification de la personne concernée, les données en question ne sont pas considérées comme anonymes. Pour garantir le caractère anonyme de ces données, il est indispensable de prendre des mesures supplémentaires (par ex. chiffrer ou généraliser certains autres renseignements). Conformément au Message du 23 mars 1988 concernant la loi fédérale sur la protection des données, on entend par "anonymisation" toute mesure visant à empêcher l'identification de la personne concernée ou à ne rendre celle-ci possible qu'au prix d'efforts démesurés (anonymisation de fait). Ces efforts doivent être tels que personne ne voudrait raisonnablement les déployer pour établir l'identité de certaines personnes. Enfin, on ne peut constater de manière abstraite mais uniquement concrètement si un ensemble de données peut être considéré comme rendu anonyme car cela dépend des autres conditions-cadres.

10. Droit de bail

Formulaires d'inscription pour locataires

La recommandation concernant les données recueillies auprès de personnes intéressées à la location d'un logement a été rejetée par divers bailleurs. Nous avons soumis le cas à la Commission fédérale de la protection des données pour décision.

Nous avons déjà abordé ce problème dans nos deux premiers rapports d'activités (p. 141 ss et 154 ss). En novembre 1994, nous avons émis une recommandation s'adressant à tous les bailleurs de Suisse. Cette recommandation a été remise aux bailleurs qui avaient participé à la procédure de consultation préalable et simultanément publiée dans la Feuille fédérale. Divers bailleurs ont rejeté la recommandation. Nous avons donc soumis le cas en février 1995 à la Commission fédérale de la protection des données pour décision. Après un échange de correspondance avec nos services sur la question de la qualité de partie des personnes qui avaient rejeté la recommandation, cette commission a décidé, en décembre 1995, qu'elle n'entrerait en matière que sur le recours d'une seule partie, l'un des plus grands bailleurs de Suisse. La décision de fond devrait nous parvenir prochainement.

II. CONTRÔLES DU PFPD

1. La nouvelle carte d'identité CI 95

La nouvelle carte d'identité suisse, émise sous format de carte de crédit plastifiée, est disponible depuis le 1er juillet 1994. Une ordonnance du Conseil fédéral en règle l'établissement; elle fixe également les conditions strictes de traitement des informations personnelles. Nous avons décidé de procéder à un contrôle portant sur le respect de ces exigences de protection des données. Débuté en octobre 1995, ce contrôle est en cours auprès de l'Office fédéral de la police.

L'ordonnance du Conseil fédéral relative à la nouvelle carte d'identité suisse "CI 95" est entrée en vigueur le 1er juillet 1994. Cette ordonnance règle non seulement la procédure d'établissement de cette nouvelle carte d'identité produite sous format de carte de crédit plastifiée, mais elle fixe également de manière très précise les conditions de traitement des données personnelles collectées à cet effet. En outre elle contient, suite à notre demande, de nombreuses dispositions restrictives en matière de protection des données.

Dans le cadre de nos compétences de surveillance, nous avons décidé de procéder à un contrôle portant sur le respect de ces exigences et avons pris contact avec l'organe responsable de la banque de données relative à la nouvelle carte d'identité. Il s'agit de la section de la police administrative, au sein de l'Office fédéral de la police.

Cet examen, débuté en octobre 1995 est encore en cours. Il porte notamment sur le contenu et le caractère isolé de la banque de données gérée par l'Office fédéral de

la police, les autorisations d'accès à ce système, la saisie des données, leur transmission au producteur de la carte et à l'Office fédéral de la police, le traitement des données, leur destruction à l'échéance de la durée de conservation, l'utilisation du code lisible par machine ou encore sur les informations contenues sur la carte d'identité elle-même.

2. Le système d'information de l'Institut suisse de pédagogie professionnelle

L'Institut suisse de pédagogie professionnelle dispose d'un système de traitement des données qui gère l'administration des cours, la formation de base, ainsi que l'organisation de séminaires et de colloques pour les enseignants. Nous avons contrôlé ce système afin de vérifier si les mesures nécessaires à un traitement des données conforme à la protection des données et les mesures nécessaires de sécurité des données ont été prises.

La loi fédérale sur la formation professionnelle et l'ordonnance sur l'Institut suisse de pédagogie professionnelle sont les bases légales permettant l'utilisation d'applications informatiques pour gérer rationnellement la formation professionnelle. Le système dont il est ici question renferme les données personnelles d'environ cinq mille personnes (participants aux cours, chargés de cours, auteurs d'exposés, élèves ayant achevé leur formation, enseignants). Les divers traitements de données sont essentiellement effectués pour permettre le déroulement optimal de la formation continue d'enseignants à temps complet et à temps partiel.

Nous avons contrôlé les diverses procédures de traitement du système, les diverses possibilités de traitement des données (archivage, communication, etc.) et les mesures de sécurité quant à l'accès aux locaux et aux données.
Nous avons à cette occasion constaté qu'il n'y avait pas de traitement illicite des données et que les mesures garantissant la sécurité des données étaient suffisantes.

3. Fichier des journalistes à Zermatt

Alertés par le Conseil de presse de la Fédération suisse des journalistes de l'existence d'un fichier des journalistes à Zermatt, nous avons procédé aux éclaircissements nécessaires. Nous avons vérifié si le traitement de données en cause était susceptible de porter atteinte à la personnalité d'un nombre important de personnes et si le fichier devait être enregistré. Nous avons conclu que ce fichier ne violait pas les dispositions de la loi fédérale sur la protection des données. L'existence d'une liste noire n'a finalement pas été établie.

L'office du tourisme de la commune de Zermatt gère une banque de données où sont enregistrées des données relatives à quelque 4500 journalistes. Le but de ce fichier est l'optimisation des contacts avec les médias. La banque de données permet l'enregistrement des données suivantes : "nom", "prénom", "adresse", "date de naissance" (pas utilisée), "nationalité", "domaine de spécialisation", "activité de journaliste" (TV, Radio, presse écrite...), "statut journalistique" (journaliste libre, rédacteur, ...), "date de la visite à Zermatt", "était-il accompagné et par qui", "qui au sein de l'office du tourisme l'a pris en charge", "quel soutien a-t-il reçu lors de son

séjour", "a-t-il été invité à manger", "où et quel était le menu", "a-t-il reçu une carte de libre parcours", "a-t-il reçu un cadeau", "qui a réservé l'hôtel" et "qui a payé la facture", "a-t-il écrit sur Zermatt", "l'article était-il positif pour Zermatt", "a-t-il été remercié", "quelles informations a-t-il demandées" et "quelle documentation lui a-t-on remise". Ces informations se limitent uniquement au travail journalistique durant le séjour à Zermatt et ne concernent pas la vie privée du journaliste. Les données relatives au restaurant ou au menu ne sont collectées que pour éviter d'inviter une personne deux fois au même endroit et de lui offrir le même menu. Il en va de même pour les éventuels petits cadeaux que l'office offre de temps à autre. Les informations sur les réservations d'hôtel, facturation ou accompagnement à Zermatt sont de nature purement administrative (logistique, comptabilité). Pour chaque article ou reportage, l'office du tourisme peut attribuer une note entre 1 et 5 (excellent, bon, moyen, Zermatt pas mentionné, aucune valeur pour Zermatt). Ces notes se réfèrent non à la qualité de l'article ou du reportage, ni à des jugements positifs ou négatifs, mais à l'impact sur la station. Elles ne qualifient pas le journaliste en tant que personne.

Les données enregistrées ne sont pas communiquées et le droit d'accès des journalistes concernés est garanti.

Dans la mesure où les principes généraux du traitement de données personnelles sont respectés, l'office du tourisme peut faire valoir un motif justificatif au traitement de données sur les journalistes qui sont en contact avec lui. Sur la base de nos observations et des informations en notre possession, nous avons constaté la licéité de la collecte et du traitement des données, la finalité ressortant des circonstances du traitement, et les journalistes ayant connaissance du traitement.

Pour ces motifs, nous avons conclu que la banque de données sur les journalistes de l'office du tourisme de Zermatt ne viole pas la loi fédérale sur la protection des données et que le fichier ne doit pas être annoncé en vue de son enregistrement. Il a cependant été recommandé de garantir l'exactitude des données et leur actualité, notamment en détruisant les données relatives aux journalistes, au plus tard cinq ans après leur dernier contact avec Zermatt. L'office du tourisme a également été invité à informer expressément les journalistes de l'existence du fichier et de leur droit d'accès.

4. Vidéosurveillance aux postes frontières

La surveillance de la frontière verte au moyen d'appareils vidéo est régie par une ordonnance du Conseil fédéral. Les enregistrements effectués sont nécessaires pour garantir la sécurité de la ligne des douanes et la perception des droits et pour surveiller le franchissement de la frontière. Les enregistrements doivent être effacés dans les 24 heures. Nous avons procédé à un contrôle d'une installation vidéo à la frontière.

A la fin de l'année 1991, deux caméras vidéo ont été installées au poste frontière que nous avons contrôlé. Ces caméras permettent la surveillance de deux ponts qui peuvent être franchis jour et nuit, à pied ou à vélo. Le passage est autorisé dans la mesure où les personnes sont porteuses d'une pièce d'identité en règle et ne transportent pas de marchandises au-delà des quantités légales admises. Le passage frontière est signalé, notamment par une interdiction de circuler. Les

caméras sont cachées et il n'y a aucune indication du fait que la zone est sous surveillance vidéo. Toutefois, la population locale est informée. Les deux caméras sont en fonction en permanence. Elles enregistrent cependant les passages uniquement lorsqu'une personne ou un animal franchissent les ponts. Deux installations différentes sont testées. L'une recourt à un magnétoscope et permet d'enregistrer chaque passage sur une bande vidéo. Cette bande une fois pleine est effacée et réutilisée jusqu'à usure, puis détruite et remplacée. Elle peut être revisionnée avant d'être effacée. Cela porte généralement sur les dernières minutes et peut remonter parfois aux deux ou trois dernières heures d'enregistrement au maximum. Au-delà, cette opération devient inutile. La deuxième caméra est reliée à un disque dur. Ce système permet uniquement l'enregistrement des deux dernières images qui sont automatiquement effacées lors du passage suivant. Les deux systèmes ne permettent pas d'imprimer ou de développer des photos. Deux moniteurs de contrôle sont installés dans le poste de douane et permettent aux douaniers de suivre les mouvements et le cas échéant d'intervenir.

La vidéosurveillance est régie par l'ordonnance du 26 octobre 1994 réglant la surveillance de la frontière verte au moyen d'appareils vidéo. Celle-ci permet l'installation d'appareils vidéo pour garantir la sécurité de la ligne des douanes et la perception des droits et pour surveiller le franchissement de la frontière. L'utilisation des caméras contrôlées respecte ces finalités. La signalisation du passage de la frontière sur les ponts est suffisante compte tenu des lieux et permet aux personnes concernées de savoir qu'elles franchissent la frontière et s'exposent de ce fait à un contrôle. En ce qui concerne la durée de conservation des données limitée à 24 heures, nous avons constaté que le système du disque dur respecte cette exigence légale, puisque les images sont effacées au fur et à mesure des différents passages. Le système avec bande vidéo ne respecte en revanche pas ces exigences puisque l'effacement intervient au plus tôt 36 heures après le 1er enregistrement. Du point de vue de l'efficacité du travail des douaniers et compte tenu du nombre de passages enregistrés, le système avec bande vidéo est cependant préférable. Encore faut-il, pour qu'il soit compatible avec la protection des données, que l'effacement intervienne dans les 24 heures. En ce qui concerne la sécurité des données, nos n'avons pas décelé de lacunes particulières.
Suite au contrôle, nous avons proposé aux autorités douanières d'utiliser des bandes de courte durée pour garantir l'effacement des données dans les 24 heures. Cette proposition a été acceptée.

5. Service des renseignements des Télécom Genève (no 111)

Nous avons effectué en janvier 1996 un contrôle auprès du service des renseignements des Télécom Genève. Nous avons examiné si les employés avaient été dégagés de l'obligation de s'annoncer en mentionnant également leur prénom et si les évaluations de comportement par écoute étaient conformes à la protection des données.

Nous avons tout d'abord examiné si suite à une intervention de notre part (cf. 144), les employés des renseignements avaient été dégagés de l'obligation de se présenter en mentionnant également leur prénom. Les employés interrogés ont dit qu'ils se sentaient libres de ne pas mentionner leur prénom et étaient heureux que cette obligation ait été supprimée.

Nous avons ensuite enquêté sur la conduite d'évaluations du comportement au moyen d'écoutes téléphoniques faites à l'improviste par les supérieurs. La réalisation de ces évaluations est réglementée en détail dans une directive de la Direction générale des PTT. Une fois ou plus par an, la communication de renseignements par les téléopératrices est enregistrée durant environ 45 minutes par les supérieurs et l'enregistrement est ensuite discuté avec la personne concernée. Il a pour but de détecter et corriger les fautes commises durant la communication des renseignements, de contrôler l'amabilité et la rapidité de cette même communication et d'apprécier les bonnes prestations. Tant selon les opératrices que selon leurs supérieurs, les écoutes satisfont à ces objectifs. Mais du point de vue de la protection des données, deux problèmes se posent : d'une part les écoutes ne reposent sur aucune base légale, d'autre part elles se font sans avertissement. Aussi les téléopératrices interrogées souhaitent-elles que les écoutes soient annoncées au préalable. Notre contrôle a montré que l'écoute se limite à la communication de renseignements, et que les conversations privées entre téléopératrices ne sont pas enregistrées. En outre, les écoutes se déroulent dans l'ensemble conformément aux règles de la Direction générale des PTT (évaluer l'écoute avec la personne concernée, remplir une feuille d'appréciation, conservée jusqu'à la prochaine qualification puis détruite, effacer l'enregistrement immédiatement après l'appréciation). La Directive requiert toutefois l'effacement en présence de la personne concernée, ce qui n'est pas le cas à Genève, et l'information du personnel sur le but et l'exécution de l'évaluation de la prestation, ce qui n'est pas toujours le cas. Nous avons donc conseillé aux Télécom Genève d'informer systématiquement le personnel, à l'occasion de son engagement et de sa formation, sur le but, le contenu et la réalisation des évaluations de prestations, d'annoncer au prélable l'écoute et de l'effacer systématiquement en présence de la personne concernée. Parallèlement, nous sommes intervenus auprès de la Direction générale des PTT afin d'éclaircir dans quelle mesure la création d'une base légale serait utile et opportune dans l'optique de la future privatisation des Télécom.

III. AUTRES THEMES

1. Protection des données et conditions légales cadres

1.1. Transposition des exigences de la LPD dans le cadre de la législation

Selon la LPD, des bases légales au sens formel doivent être créées ou adaptées d'ici le 1er juillet 1998 pour les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité. Sur demande du Secrétariat général du DFJP, nous avons présenté dans un avis de droit les dispositions particulières qui devaient être édictées.

D'après l'article 38, 3e alinéa, LPD, les organes fédéraux doivent créer d'ici le 1er juillet 1998 des bases légales formelles pour les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité. Ils doivent en revanche élaborer immédiatement les bases légales requises en cas de création ou d'extension notoire de tels fichiers. La question de savoir ce qui devait être réglé et comment a fait l'objet d'un avis de droit que le PFPD a rendu en automne 1995

après discussion avec l'Office fédéral de la justice, et qui devrait être publié dans la jurisprudence des autorités administratives de la Confédération (JAAC). Les points suivants doivent principalement être retenus :

- si des données sensibles ou des profils de la personnalité sont traités régulièrement, il faut le signaler dans une loi au sens formel. Dans ce contexte, le but et l'importance du traitement des données, les moyens utilisés ainsi que l(es) autorité(s) habilitée(s) à procéder au traitement doivent être déterminés avec suffisamment de précision.
- Si, pour le traitement des données, l'on fait appel à un système TED important et à larges ramifications ("moyens utilisés"), dans lequel sont traités dans une mesure importante et par différentes autorités des données personnelles, notamment des données sensibles et des profils de la personnalité, il faut le mentionner expressément dans une loi au sens formel.
- Si des données personnelles, notamment des données sensibles ou des profils de la personnalité doivent être régulièrement échangés entre différentes autorités à des fins de traitement diverses, cela doit figurer expressément dans une loi au sens formel. Si différentes autorités ont accès à ces données par procédure d'appel, il faut aussi que cela soit mentionné expressément, de même que l'autorité autorisée à le faire. Si des échanges réguliers sont effectués avec des autorités de l'étranger, cela doit également être réglé expressément.
- S'il apparaît que certaines atteintes aux droits fondamentaux découlant du traitement des données ne sont conformes à ces droits qu'en relation avec des mesures de protection concrètes et spécifiques au domaine traité, ces charges, respectivement les limites apportées aux atteintes envisagées doivent être formellement réglées par la loi. Les dispositions relatives aux mesures de surveillance des personnes par des moyens techniques et leurs limites, c'est-à-dire leur contrôle dans la loi fédérale sur la procédure pénale (articles 65ss PPF), ou les dispositions relatives à la protection des données de tiers non concernés lors de l'interrogation du RCE à des fins d'identification dans le cadre d'une poursuite pénale (article 7, 3e alinéa, de l'ordonnance sur le RCE, dont le contenu a été accepté dans le projet décidé par le Conseil fédéral pour la révision de la LSEE) en sont des exemples.

Maintenant que cet avis de droit existe, il s'agira dans une étape ultérieure d'entreprendre les travaux législatifs nécessaires si ce n'est pas encore fait. Sur demande et en collaboration avec l'Office fédéral de la justice, nous nous tiendrons à disposition des organes fédéraux concernés pour les conseiller dans le cadre de notre mandat légal.

1.2. Projet de loi fédérale sur les armes, les accessoires d'armes et les munitions

Consultés sur ce projet législatif à différents stades de son élaboration, nous avons mis en évidence la nécessité de réglementer plus clairement les nombreux traitements de données personnelles qu'impliquera l'application de cette loi. L'Office fédéral de la police, après avoir introduit dans ce projet un grand nombre de dispositions de délégation de compétence au Conseil fédéral, a suivi notre proposition en élaborant également une norme de délégation spécifique au traitement des données.

Dans le cadre de la procédure de consultation ouverte par l'Office fédéral de la police, et concernant l'avant-projet de loi fédérale sur les armes, les accessoires d'armes et les munitions, nous avons relevé en mai 1995 l'important travail de traitement de données personnelles imposé aux différents intervenants. Nous avons notamment demandé l'introduction de précisions dans la loi, en particulier quant à la collecte d'informations liée aux obligations de vérification d'identité, à la tenue d'une comptabilité ou à l'octroi de permis. De même, nous avons demandé à ce que soient élaborées des dispositions claires concernant les nombreux communications et échanges de données prévus entre aliénateurs privés, autorités cantonales, fédérales et étrangères compétentes.

Il est ressorti de la publication des résultats de cette procédure de consultation, en septembre 1995, que les prises de position des offices concernés, notamment nos observations, ont été prises en considération. Toutefois, à nouveau consultés en novembre 1995 sur le projet de loi remanié et son projet de message, nous avons constaté que nos remarques et propositions relatives aux activités de collecte, de communication et de traitement de données n'ont été que peu ou pas retenues. En outre, bien que le nouveau projet prévoie un grand nombre de normes de délégation de compétence au Conseil fédéral, aucune d'entre elles ne traitait clairement de la protection de données.

Prenant position sur ce nouveau projet, nous avons pris acte qu'aucune communication de données sensibles ou de profils de la personnalité au moyen d'une procédure d'appel (liaison online) n'est prévue. Nous avons d'autre part rappelé que toute communication de données personnelles au moyen d'une procédure d'appel doit le cas échéant être expressément mentionnée dans l'ordonnance d'application. Enfin, nous avons relevé qu'en ce qui concerne le traitement des données personnelles, la délégation de compétence au Conseil fédéral ne ressort pas suffisamment clairement du projet. Nous avons donc exigé que soit intégrée une disposition générale de délégation de compétence en matière de protection des données. Cette norme doit prévoir que le Conseil fédéral règle par voie d'ordonnance les modalités des traitements de données effectués en application de la présente loi, les autorisations d'accès aux données et leurs durées de conservation. S'inspirant de notre proposition, l'Office fédéral de la police a élaboré et introduit la norme de délégation de compétence requise dans la version finale du projet de loi. Ce dernier a été approuvé en janvier 1996 par le Conseil fédéral et transmis pour examen au Parlement.

1.3. Avant-projet de loi fédérale concernant la procréation médicalement assistée et instituant une Commission nationale d'éthique - consultation des milieux intéressés

Dans le cadre de la procédure de consultation des milieux intéressés, nous avons adressé un premier avis à l'Office fédéral de la justice. La nécessité d'alléger, pour les futurs parents, les procédures de consentement lors du recours à la procréation médicalement assistée, a en particulier été soulignée. Nous avons au demeurant émis des doutes quant à l'opportunité, tant du point de vue scientifique que pour le bien de l'enfant à venir, de prévoir la possibilité de sélectionner le sperme d'un donneur en fonction de sa ressemblance physique avec le futur père. Nous avons également estimé que des informations telles que l'état civil, la religion, la profession

et la formation du donneur ne sont pas nécessaires à l'enfant désireux de connaître son ascendance biologique. Il a finalement été signalé qu'un délai de conservation des données de 80 ans est excessif.

2. Communication de données personnelles

2.1. Communication de données personnelles à des tiers au sens de l'article 11, 3e alinéa LPD

Les personnes privées qui communiquent des données personnelles à des tiers sont tenues de déclarer le fichier concerné au Préposé fédéral à la protection des données si le traitement de ces données n'est soumis à aucune obligation légale ou si les personnes concernées n'en ont pas connaissance. Dans des cas d'espèce, il faut vérifier si le destinataire des données est considéré comme un tiers au sens de l'art. 11, 3e alinéa, LPD.

Une personne privée s'est adressée à nous pour savoir si les données de clients traitées sur mandat par une imprimerie devaient nous être annoncées. On ne peut pas répondre de manière générale à cette question, car pour savoir s'il s'agit d'une communication de données à des tiers au sens de l'article 11, 3e alinéa, LPD il faut déterminer de cas en cas le genre de données personnelles et les circonstances de leur communication. On entend par communication le fait de rendre accessibles des données personnelles par consultation, transmission ou publication. Dans ce contexte, il s'agit notamment d'examiner :

- quel genre de données personnelles sont traitées;
- si le tiers est une personne indépendante ou s'il se trouve dans un rapport de subordination avec le maître du fichier;
- dans quel but les donnés sont transmises à des tiers;
- comment les données sont traitées par les tiers, notamment si le tiers transmet les données personnelles à d'autres personnes;
- si le destinataire est intéressé à titre primaire au contenu des données ou s'il ne traite que techniquement les données pour les rendre ensuite dans leur totalité au maître du fichier.

Si le maître d'un fichier confie par exemple à une imprimerie le mandat d'imprimer des formules pour la distribution d'ordres de paiement, des données personnelles sont transmises à l'imprimerie. Dans ce cas, l'imprimerie ne reçoit les données des clients que pour un traitement technique et ne peut traiter les données que conformément au mandat confié. Le traitement des données personnelles par l'imprimerie se termine lorsque les ordres de paiement sont imprimés, raison pour laquelle ces données sont retournées dans leur intégralité au mandant. Dans ce contexte, la communication des données sert uniquement de moyen pour permettre au mandant de poursuivre ses tâches ultérieures. Ainsi, l'imprimerie n'est que la destinataire des données personnelles, et non pas un tiers au sens de l'article 11, 3e alinéa, LPD. Il n'est donc pas nécessaire de nous annoncer le fichier.

2.2. Communication de données relatives aux boursiers étrangers

La création, par un organe fédéral, d'une banque de données aux fins de communication et de publication de données relatives aux bénéficiaires étrangers de bourses d'étude doit reposer sur une base légale suffisante, se limiter aux seules finalités poursuivies par la publication des données et respecter le droit de la personne concernée de s'opposer à la publication ou à la communication.

En matière d'attribution de bourses à des étudiants et artistes étrangers, nous avons souligné qu'en l'absence de base légale prévoyant la création et la gestion d'une banque de données accessible aux tiers, et sans dispositions légales de communication des données, un organe fédéral ne peut effectuer une telle communication que sur demande et dans un cas d'espèce. Encore faut-il que la personne concernée ait donné son consentement, ou que la communication se limite uniquement aux nom, prénom, adresse et date de naissance de l'intéressé. La communication est également possible si la personne concernée a elle-même rendu ses données accessibles à tout un chacun.

Quant à la communication systématique et régulière de données, notamment la communication sous forme de listes, la publication de brochures ou la mise à disposition par procédure d'appel (accès en ligne), elle nécessite l'adoption préalable d'une base légale suffisante. En particulier, si l'accès aux données se fait par procédure d'appel, il doit être prévu expressément. La communication de données relatives aux boursiers doit en outre être facultative. Chaque bénéficiaire de bourse doit avoir la possibilité de refuser de figurer dans la banque de données ou de voir communiquer les données le concernant. Enfin, le catalogue des données rendues accessibles à tout un chacun doit se limiter aux seules données nécessaires aux finalités poursuivies par la publication ou la diffusion.

2.3. Entraide administrative par communication de listes en droit des subventions, droit fiscal et droit de l'environnement

Les organes fédéraux n'ont le droit de communiquer des données personnelles au moyen de listes à des fins autres que celles prévues lors de la collecte que si des bases légales existent. Dans deux cas qui nous ont été soumis, ces conditions n'étaient pas remplies, raison pour laquelle nous n'avons pas pu donner notre accord à la transmission des données envisagée.

Dans deux avis, nous nous sommes exprimés au sujet de la transmission, dans le cadre de l'entraide administrative, de listes importantes de données personnelles. Dans le premier cas, l'Administration fédérale des finances a demandé à l'Office fédéral de l'agriculture de lui transmettre la liste de tous les destinataires de contributions de fermeture d'entreprises. Dans le deuxième cas, une chambre de commerce étrangère a prié la Commission Suisse Interdisciplinaire pour la Sécurité biologique dans la Recherche et dans ses Applications Techniques de lui communiquer les entreprises actives dans la recherche génétique annoncées selon l'ordonnance sur la protection contre les accidents majeurs.

Ni le droit agricole, ni le droit fiscal ou le droit de la protection de l'environnement ne prévoient la communication à grande échelle de données à des tiers (autorités ou personnes privées), à des fins étrangères à celles de la collecte. Dans de tels cas, les données ne peuvent être communiquées que dans des cas d'espèce.

Concrètement, en matière fiscale, il aurait en outre fallu rendre vraisemblable le fait que les personnes concernées avaient eu un comportement contraire au droit. Dans le cas des entreprises de recherche génétique, il aurait fallu prouver leur accord. Ces conditions n'étant pas non plus remplies, notre réponse a été négative.

3. Flux transfrontières

Flux transfrontières de données au sein d'une multinationale et obligation de déclarer

Au cours de l'exercice écoulé, de nombreuses sociétés nous ont contactés pour savoir dans quelles conditions elles étaient en droit de transmettre leurs données à l'étranger. Il s'agissait dans la plupart des cas de sociétés multinationales désirant transmettre à la maison-mère ou au siège principal sis à l'étranger des données concernant leurs collaborateurs, en vue de restructurations effectuées au niveau mondial, de la planification d'une succession ou d'une mutation interne efficace au sein même du groupe.

Pour fonctionner de manière rationnelle et efficace, les entreprises multinationales doivent pouvoir échanger des données entre leurs différentes succursales. Il s'agit essentiellement de données concernant les collaborateurs des succursales ou filiales qui sont transmises au siège principal ou à la maison-mère. Elles sont destinées à la mise en oeuvre efficace des ressources humaines disponibles dans l'entreprise et à la planification optimale des successions. Ce sont la plupart du temps des données personnelles se rapportant aux cadres moyens et supérieurs.
Les flux transfrontières de données peuvent menacer la personnalité des individus concernés, notamment en raison du manque de clarté des transmissions à l'étranger. En effet, à partir du moment où les données se trouvent à l'étranger, la personne concernée ne peut plus guère faire valoir ses droits d'accès et de rectification, surtout dans des Etats sans protection des données équivalente à la nôtre, ce qui ne fait qu'augmenter le danger d'atteinte à la personnalité du fait, par exemple, d'un traitement non autorisé des données ou d'un traitement de données inexactes.

Pour ces raisons, nous attirons ici votre attention sur les éléments essentiels qui sont à observer lors de transmissions de données à l'étranger :

Qui porte la responsabilité des transmissions de données à l'étranger ?

La loi suisse sur la protection des données ne prévoit pas de procédure spécifique d'autorisation pour les transmissions de données à l'étranger. Des données personnelles peuvent être transmises à l'étranger lorsque la personnalité de la personne concernée ne s'en trouve pas gravement menacée. Le législateur a sciemment laissé à la personne opérant la transmission la responsabilité et l'appréciation des risques d'une telle communication.

L'obligation de déclarer prévue par la loi pour certaines transmissions à l'étranger ne libère pas le maître d'un fichier de sa responsabilité : il doit veiller au respect des règles matérielles de la loi. Le maître du fichier doit apprécier lui-même le risque d'une atteinte à la personnalité exactement de la même manière que pour un fichier non soumis à déclaration.

But de l'obligation de déclarer

La déclaration de transmissions à l'étranger vise la transparence du traitement des données. Le PFPD veille par interim aux droits des personnes dont les données personnelles sont transmises à l'étranger. C'est la raison pour laquelle il n'y a pas d'obligation de déclarer lorsque les personnes concernées ont connaissance de la transmission des données.

Quand est-on obligé de déclarer une transmission à l'étranger ?

- Lorsque le *fichier** quitte le territoire national suisse, ou
- lorsque les données peuvent être consultées de l'étranger, ou
- lorsque les données sont transmises à un tiers chargé de traiter les données pour le compte de la personne opérant la transmission.

* On entend par *fichier* tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.

Le point important est que les données quittent le territoire suisse et non que les données soient transmises à l'intérieur d'une société ou d'un groupe.

Quand n'est-on pas obligé de déclarer une transmission ?

- Lorsque la communication repose sur une obligation légale, ou
- lorsque les personnes concernées ont *connaissance** de la transmission de données.

* Il y a *connaissance* des personnes concernées lorsqu'au moins le maître du fichier, les données transmises, le but de la transmission à des tiers et le pays de destination des données sont connus.

Exceptions à l'obligation de déclarer

- La transmission de données à des fins ne se rapportant pas à des personnes (statistique, planification, recherche) ne doit pas être obligatoirement déclarée dans la mesure où la publication des résultats ne permet pas une identification des personnes concernées.
- Les transmissions de données dans des pays possédant une protection des données équivalente à celle du droit suisse doivent être obligatoirement déclarées seulement lorsqu'il s'agit de données sensibles ou constitutives des *profils de la personnalité**.

* Dans le cas de transmissions entre entreprises et groupes en vue d'une mise en oeuvre efficace des ressources humaines, il s'agit d'informations représentatives qui constituent souvent des *profils de la personnalité*.

La procédure de déclaration

Lorsqu'une transmission à l'étranger doit être déclarée, il faut fournir les renseignements suivants (le formulaire nécessaire est disponible gratuitement auprès du Secrétariat du PFPD) :

- nom et adresse de la personne qui communique les données personnelles;

- nom et adresse du destinataire des données;
- nom et dénomination complète du fichier;
- catégories de données personnelles communiquées;
- cercle et nombre approximatif des personnes concernées;
- but du traitement des données par le destinataire;
- genre et fréquence des communications;
- date de la première communication.

Contrairement aux fichiers soumis à déclaration, les déclarations de flux transfrontières ne sont ni enregistrées, ni publiées.

Il convient en particulier de veiller aux points suivants en cas de transmissions de données à l'étranger :

- Déterminez tout d'abord la situation juridique du pays destinataire.
  Consultez en premier lieu la liste des Etats possédant une protection des données équivalente à celle de la Suisse. Cette liste est disponible auprès du PFPD. Si le pays destinataire ne dispose pas d'une protection des données équivalente ou s'il demeure des incertitudes sur la situation juridique, il est recommandé de conclure avec le destinataire un arrangement contractuel afin de garantir un niveau de protection des données équivalent à celui de la Suisse. Cet arrangement règlementera au moins :
- la définition précise et obligatoire de l'usage prévu
- le droit d'accès des personnes concernées
- la règlementation de la sécurité des données selon le degré de sensibilité des données
- les conséquences, au cas où le destinataire ne remplit pas ses obligations (dommages-intérêts ou peine conventionnelle).

- Assurez-vous que les données transmises sont correctes

- Prenez les mesures techniques nécessaires à la transmission (sécurité des données) pour protéger les données contre leur perte ou contre l'accès de personnes non autorisées.

Le Conseil de l'Europe a élaboré un contrat-type qui peut être utilisé pour la réglementation des flux transfrontières de données (cf. annexe p. 215; la version anglaise peut également être obtenue auprès de notre Secrétariat).

4. Protection et sécurité des données

4.1. Exigences de la protection des données en bureautique

Des ordinateurs performants mis en réseau et équipés de logiciels adéquats offrent de toutes nouvelles possibilités dans le domaine de la bureautique. Ils peuvent ainsi contribuer à rendre bien plus simples les déroulements administratifs. Il est cependant important de ne pas oublier que certaines mesures de précaution doivent être prises lorsqu'on traite des données personnelles.

La bureautique est au service du travail de bureau, elle facilite ainsi la création, la mise à jour, l'archivage, la recherche et la distribution d'informations sous forme de textes, de données, d'images ou de messages vocaux. Les postes de travail dans les bureaux sont équipés d'ordinateurs de plus en plus performants et sont souvent interconnectés dans un réseau, ce qui permet d'élargir grandement l'étendue des données qui peuvent être traitées, en allant du simple traitement de texte à l'application sophistiquée de «groupware».

Dans le cadre d'un groupe de travail qui s'est occupé de la sécurité dans l'environnement bureautique de l'administration fédérale, nous avons attiré l'attention sur

les exigences principales qui doivent être remplies du point de vue de la protection des données. Nous en résumons quelques-unes ci-dessous :

- le principe selon lequel le traitement de données personnelles par des organes fédéraux doit reposer sur une base légale est en particulier également applicable à la bureautique.
- Des mécanismes de contrôle adéquats doivent garantir qu'une manipulation non autorisée de documents soit impossible. Toutes les modifications doivent être reproductibles.
- Certaines données ne peuvent être consultées que dans le but nécessaire à l'accomplissement de la tâche concrète, respectivement dans le but fixé dans les bases légales.
- Les systèmes bureautiques permettent souvent d'accéder à des données provenant de plusieurs sources (qui individuellement ne posent pas de problème). Des mesures techniques doivent garantir qu'il est impossible à des personnes non autorisées d'effectuer de manière automatique des liens entre ces données, car de tels liens permettent finalement de constituer des profils de la personnalité.
- La transmission de documents, sous quelque forme que ce soit, doit être soumise à un contrôle. Il doit être possible de connaître aussi bien l'expéditeur que le destinataire. Les documents doivent être protégés de manière appropriée contre toute atteinte à leur intégrité et à leur confidentialité.
- Les données personnelles qui ne sont plus utilisées doivent être rendues anonymes ou détruites, à moins qu'elles ne doivent être conservées à titre de preuve, par mesure de sûreté ou être déposées aux Archives fédérales.

L'étendue des fonctions ainsi que l'énorme souplesse des systèmes bureautiques fait qu'il est très difficile de remplir ces exigences uniquement à l'aide de moyens techniques. Une des mesures appropriées et efficace est cependant la journalisation des traitements. Bien qu'elle n'empêche pas directement un traitement non autorisé, elle permet néanmoins de vérifier par la suite la légitimité du traitement et surtout sa finalité. Parallèlement, des mesures organisationnelles adaptées à l'environnement concret doivent être prises.
En règle générale, on ne sait pas à l'avance quelle est la sensibilité des données qui seront traitées dans les systèmes bureautiques, c'est pourquoi le choix des mesures à prendre doit en cas de doute s'orienter en fonction du cas le plus défavorable.

4.2. Enregistrement online de logiciels

Lorsqu'un éditeur de logiciels permet d'enregistrer le logiciel acquis directement par l'intermédiaire d'un modem, il doit garantir que le client ait connaissance de toutes les données qui sont transmises. Il doit être techniquement possible d'empêcher la transmission.

De plus en plus de logiciels pour PC permettent un enregistrement online (en ligne) par modem comme alternative à l'envoi de la carte d'enregistrement par courrier postal. Cette possibilité est également offerte aux acquéreurs de Windows95, le système d'exploitation pour PC que la société Microsoft a mis sur le marché l'an passé. Certains articles de presse de même que des personnes privées qui nous ont contactés ont fait part de leur crainte que la société Microsoft enregistre

éventuellement des données en provenance du PC du client sans que ce dernier en soit informé. Nous avons décidé d'examiner la chose de plus près, de telles méthodes étant susceptibles de porter atteinte à la personnalité d'un grand nombre de personnes.

Le résultat de nos recherches n'est pas encore connu au moment où ce rapport va sous presse. Nous sommes néanmoins en mesure de faire aujourd'hui déjà les déclarations d'ordre général suivantes :

la collecte licite de données personnelles ainsi que leur traitement conforme au principe de la bonne foi sont des principes fondamentaux de la protection des données. Il en découle qu'en aucun cas des données personnelles en provenance d'un PC ne peuvent être transmises à un éditeur, à une société de logiciels, etc. sans que l'utilisateur le sache ou puisse le cas échéant l'accepter. Il doit savoir quelles sont les données transmises et avoir la possibilité d'empêcher leur transmission en tout ou en partie.

4.3. Responsabilité du mandant et de l'entreprise prestataire lors de prestations de services dans le domaine informatique

Lorsqu'une personne remet à un fournisseur un disque dur contenant des données personnelles pour réparation, elle est tenue avant tout de respecter les mesures de sécurité des données garantissant la confidentialité des données, surtout lorsque ce disque dur est envoyé à l'étranger. D'autre part, la maintenance (à distance) de systèmes informatiques nécessite également que des mesures adéquates soient prises au niveau technique et organisationnel.

Personne ne cède volontiers des données en provenance de son environnement personnel ou des données sensibles s'il n'est pas sûr que ces données seront bel et bien traitées de manière confidentielle.

Le maître d'un fichier doit veiller à ce qu'un tiers ne traite les données que dans la même mesure que celle dans laquelle il est lui-même autorisé à le faire. La cession du droit de traitement à des tiers n'est en outre autorisée que si elle n'est pas interdite par une clause (légale ou contractuelle) de maintien du secret. Une abrogation par contrat des dispositions de protection des données envers le client reste sans effet.

Lors de la réparation ou de l'échange d'un disque dur il est sans autre possible de consulter des données ou même de les transmettre à d'autres de manière incontrôlée. Un moyen d'éviter ceci consiste à encoder les données mémorisées sur le disque dur. Il faut cependant veiller à utiliser des algorithmes de codage qui ont fait leurs preuves et utilisent des clés de longueur suffisante.
Si les données stockées sur le disque ne sont pas codées, on peut les rendre confidentielles en les effaçant. Il est cependant très important de procéder à un effacement physique, par opposition à l'effacement logique qu'effectuent la majorité des systèmes d'exploitation et qui permet de reconstituer facilement les données effacées. Des utilitaires spéciaux (réécrivant le support plusieurs fois avec des valeurs différentes, etc.) permettent d'obtenir un effacement permanent des données. Si un support de données ne répond plus, il peut être traité à l'aide de puissants champs magnétiques alternants. Nous tenons à relever que si la suppression

n'a pas été effectuée dans les règles de l'art, des spécialistes sont en mesure de tirer profit du magnétisme résiduel et de rendre ainsi réversible la suppression des données.

Relevons dans ce contexte qu'il va de soi qu'il faut effectuer des copies de sécurité (back-up) des données, sans quoi la panne d'un disque dur pourrait causer la perte définitive de données et entraîner d'énormes coûts de récupération.

Souvent, des disques défectueux sont expédiés à l'étranger (par ex. à l'adresse du constructeur). Les mesures évoquées permettant d'assurer la confidentialité doivent être particulièrement appliquées dans ce cas. Les fichiers qui sont expédiés à l'étranger doivent être déclarés au préposé fédéral à la protection des données s'il n'existe pas de base légale pour la communication ou si les personnes concernées n'en ont pas connaissance. La transmission n'est pas soumise à déclaration si elle concerne des Etats qui connaissent une législation de protection des données équivalente à la nôtre, à moins que les fichiers contiennent des données sensibles ou des profils de la personnalité ou s'il est prévu de réexporter les fichiers transmis vers un Etat n'ayant pas de législation équivalente.

Lors d'une maintenance (à distance) ou lors d'une intervention sur un système informatique effectuée par un représentant du fournisseur ou constructeur, on doit théoriquement également s'attendre à ce que des données puissent être consultées ou copiées de manière incontrôlée. Les privilèges élevés dont dispose le personnel de maintenance permettent à ce dernier d'exécuter un grand nombre de fonctions du système. Dans beaucoup de cas, le mandant et l'entreprise de service sont liées par un contrat contenant une clause de maintien du secret. Une telle clause constitue certainement un bon point de départ, mais elle ne dispense pas de prendre en plus des mesures de sécurité qui permettent d'éviter ou de limiter les infractions à ces dispositions contractuelles ou légales ou tout au moins de les détecter a posteriori. Comme mesures de protection dans ce contexte, signalons le cryptage des données et la journalisation des interventions effectuées par le personnel de maintenance. Comme pour toutes les mesures de sécurité, le principe de la proportionnalité doit être respecté. Pour le traitement de données sensibles, de profils de la personnalité ou lors de traitements de données à finalités sensibles, il y a lieu d'utiliser les moyens techniques les plus modernes en matière de sécurité. Sur la base des expériences actuelles, nous pouvons dire que des entreprises renommées dépensent environ 10-15% du budget total informatique pour leurs mesures de sécurité.

4.4. Aspects de protection/sécurité des données lors de la planification de projets informatiques

La sécurité des données est un sujet auquel une attention particulière doit être vouée lors du développement de systèmes informatiques. Des mesures de sécurité correspondant au niveau de sensibilité des données traitées sont prévues. Le maître de fichier en tant que responsable de la sécurité des données dépend des conseils compétents que lui donnent les experts.

L'appréciation des risques possibles que courent les personnes concernées est un critère déterminant lorsqu'il s'agit de décider des mesures de sécurité des données

devant être prises. Le guide du PFPD relatif aux mesures techniques et organisationnelles distingue trois (respectivement quatre) niveaux de sécurité, qui vont de "pas d'atteinte particulière" à "danger pour la vie et l'intégrité corporelle" des personnes concernées. Ils aident aux concepteurs du système à décider quelles mesures doivent être prises. Des conseils détaillés ne peuvent cependant être donnés que si on connaît le projet et son environnement.

La sensibilité la plus élevée existe à partir du niveau 3. Dans ce cas il est impératif d'appliquer les derniers développements de la technique. Les risques respectivement les dangers inhérents au traitement de données du niveau 3 (et supérieur) sont définis comme suit :

Niveau 3 : / élevé
Les données à caractère personnel dont l'abus peut gravement affecter la personne concernée dans sa position au sein de la société ou dans sa situation économique; respectivement les données qui sont sujettes à un secret de fonction particulier; telles que
- les fichiers de patients;
- les données relatives au personnel;

et en particulier également les données qui sont mentionnées dans la Loi fédérale sur la protection des données (LPD) à

l'art. 3	lit. c	données sensibles;
	it. d	profils de la personnalité.

(Niveau 4 : / très élevé)
Les données à caractère personnel dont l'abus peut signifier un danger pour la vie et l'intégrité corporelle de la personne concernée, telles que
- les adresses d'hommes de liaison de la police;
- les adresses de témoins dans certaines poursuites pénales;
- les adresses de personnes menacées pour avoir exprimé leur opinion.

A notre étonnement, nous sommes encore actuellement souvent obligés de constater que les documents de planification de projets informatiques sensibles ne contiennent pas de mesures de protection des données adéquates. Comme nous l'avons déjà mentionné, il y a lieu à partir du niveau de sécurité 3 de tenir compte du développement technique lors de la mise en place de mesures de sécurité. Lors de la transmission de données par exemple, on optera pour un cryptage au niveau de l'application afin de garantir la confidentialité. Si cela ne devait pas être possible, il y a lieu d'expliquer pourquoi cette mesure ne peut pas être appliquée (appréciation de la proportionnalité). A ce sujet, relevons cependant qu'il existe de plus en plus de produits sur le marché qui offrent une sécurité des données très poussée.

Des dispositions légales sont des objectifs IMPÉRATIFS lors du développement de systèmes. C'est pourquoi les considérations relatives à la sécurité des données doivent faire partie de la planification dès le début du projet. La responsabilité de la protection des données incombe au maître du fichier, c.-à-d. aux personnes privées ou organes fédéraux qui décident du but et du contenu d'un fichier. Ces derniers ont besoin de l'appui des experts qui leur démontrent de manière reproductible quelles mesures peuvent être réalisées, quels sont leurs effets et les ressources nécessaires. Ce n'est que sur la base de cette représentation transparente que le maître du fichier sera en mesure d'assumer sa responsabilité.

5. Service de renseignements

Obligation faite au service de renseignements de l'armée de déclarer ses fichiers

La nouvelle loi sur l'armée et l'administration militaire prévoit la création d'un service de renseignements. Elle autorise le Conseil fédéral à prévoir des exceptions à l'obligation d'enregistrer les fichiers en vertu de la LPD. Le service de renseignements n'est toutefois pas délié de l'obligation d'annoncer ces fichiers auprès de notre Secrétariat.

Le service de renseignements de l'armée a pour tâche de collecter, exploiter et diffuser des informations sur l'étranger essentielles à la politique de sécurité. Selon la nouvelle loi sur l'armée et l'administration militaire, le Conseil fédéral est autorisé à prévoir à ce propos des exceptions aux prescriptions de la protection des données sur l'enregistrement des fichiers. Mais sur la base de cette disposition, l'ordonnance sur le service de renseignements délie ce dernier non seulement de l'obligation d'enregistrement, mais aussi de l'obligation de déclarer les fichiers relevant du service de renseignements.

La loi fédérale sur la protection des données (LPD) différencie clairement l'obligation d'annonce de l'obligation d'enregistrement.
La déclaration garantit au PFPD la surveillance des fichiers gérés par le service de renseignements. En vertu de la LPD, les organes fédéraux sont tenus de déclarer leurs fichiers. Les exceptions à cette obligation doivent être prévues expressément par un texte légal.

La solution choisie en définitive par le Conseil fédéral ne correspond pas entièrement aux dispositions de la LPD sur la déclaration des fichiers. La loi militaire ne prévoit aucune exception au devoir d'annonce des fichiers prescrit par la protection des données et ne libère le service de renseignements que de l'obligation d'enregistrement. L'ordonnance du Conseil fédéral prévoit néanmoins la déclaration des fichiers du service des renseignements uniquement lorsqu'il n'en découle pas de menace pour la collecte des informations. Mais même si la collecte des informations n'est pas menacée, une déclaration ordinaire des fichiers n'est pas prévue. Dans de tels cas, le Préposé fédéral à la protection des données doit être informé de l'existence de ces fichiers uniquement de manière générale.

6. Impôts

Clauses de protection des données en droit fiscal - loi sur la taxe sur la valeur ajoutée et ordonnance sur la taxe d'exemption du service militaire

Dans le domaine des dispositions fiscales internationales et nationales, on tient aujourd'hui régulièrement compte des exigences de la protection des données grâce à des dispositions spécifiques, et l'on voit dans ce contexte se dessiner un standard.

Selon la LPD, il est nécessaire de créer des bases légales au sens formel pour certains traitements de données. Dans le cadre de la procédure législative en cours, nous nous sommes fait expliquer par l'Administration fédérale des contributions les traitements de données incombant à la taxe sur la valeur ajoutée et à la taxe

d'exemption du service militaire. Il en résulte que dans les deux domaines, il est nécessaire de créer des bases légales formelles pour le traitement des données. C'est pourquoi nous avons soumis une proposition de complément dans le cadre de la procédure de consultation relative à la loi sur la taxe sur la valeur ajoutée. De même, lors de la révision de l'ordonnance sur la taxe d'exemption du service militaire, nous avons soumis des propositions qui ont été reprises par l'Administration fédérale des contributions. Une adaptation de la loi sur la taxe d'exemption du service militaire militaire est envisagée pour la prochaine révision. A cette occasion, ces propositions pourront passer du niveau d'ordonnance à celui de loi au sens formel.

Il s'agit en particulier de décrire dans les grandes lignes les traitements importants de données et les procédures organisationnelles et techniques nécessaires au maintien du secret fiscal et à la protection des données. Contrairement à ce qui se passe pour la taxe sur la valeur ajoutée, l'Administration fédérale des contributions ne tient pas de fichier central pour la taxe militaire mais en laisse l'exécution aux cantons. C'est pourquoi il est particulièrement important ici de garantir un standard minimum de sécurité pour l'ensemble du pays. Cela d'autant plus que dans le cadre de la taxe militaire, l'on traite souvent des données délicates relatives à la santé. Nous sommes heureux de constater que pour cette raison, une disposition a été prise dans l'ordonnance sur la taxe d'exemption du service militaire. Conformément à cette disposition, l'Administration fédérale des contributions peut émettre des directives sur les exigences de sécurité des données et, selon les recommandations de l'Office fédéral de l'informatique, assurer la coordination (sur l'importance de ce genre de prescriptions, cf. notre 2ème Rapport d'activités p. 176 ss).

Dans le cadre de l'OCDE, un groupe de travail conseille actuellement l'adoption d'une clause spécifique de protection des données dans le modèle de convention en vue d'éviter les doubles impositions. Nous avons signifié notre accord aux représentants suisses de ce groupe de travail.

7. Banques

Obligation de divulgation des relations bancaires par les employés de banque dans les opérations de placement et de transaction

Une banque peut prescrire à tous ses employés de divulguer leurs relations bancaires dans les opérations de transaction et de placement si cela est nécessaire au respect de son devoir de diligence et pour empêcher les affaires d'initiés.

Une personne privée a attiré notre attention sur le "Règlement pour les opérations de placement et de transaction" d'une banque qui exige la divulgation de toutes les relations bancaires par ses employés dans les opérations de transaction et de placement. Si des opérations de placement et de transaction sont effectuées auprès de banques tierces par le biais de comptes non autorisés, il y a faute grave contre le règlement et les relations de travail peuvent en subir les conséquences (jusqu'au licenciement avec effet immédiat).

Le but de ce règlement pour la publication des opérations de placement et de transaction est, d'une part, d'empêcher les affaires d'initiés et, d'autre part, de protéger les collaborateurs qui, par des opérations de transaction, peuvent entrer en conflit avec leurs propres intérêts, ceux de leurs clients ou ceux de la banque. En outre, les banques sont soumises à la surveillance de la Commission fédérale des banques et doivent contrôler ces relations bancaires dans le cadre de leur devoir de diligence.

Comme l'employeur n'a en principe le droit de traiter les données de ses employés que dans la mesure où elles concernent leur aptitude à remplir leur emploi ou sont nécessaires à l'exécution du contrat de travail, la question s'est posée de savoir jusqu'à quel point la banque devait, dans les opérations de placement et de transaction, connaître les relations bancaires des employés qui, dans leur activité, n'avaient rien à voir avec les informations du domaine financier. D'après nos investigations, il existe des interconnexions très étroites entre les différents départements de la banque concernée. C'est pourquoi (presque) chaque employé peut entrer en contact avec des informations du secteur financier.

Pour ces raisons, le recensement des relations bancaires de tous les employés dans les opérations de transaction et de placement a été qualifié de licite.

8. Vidéosurveillance

Vidéosurveillance auprès de points de collecte de déchets ménagers

Il est prévu d'installer une caméra vidéo auprès d'un point de collecte de déchets ménagers dans le but d'enregistrer les activités dans le périmètre des containers, les personnes visitant ce point de collecte, leur véhicule ainsi que leur numéro de plaque de voiture. Le but recherché est de permettre d'identifier les personnes qui utilisent ce point de collecte de manière abusive ou dans un but non conforme à l'objectif. Les containers sont situés sur le terrain du centre d'entretien de la commune.

Une société de sécurité privée chargée d'installer des équipements de surveillance est une personne privée au sens de la LPD. Dans le cas où la commune mandate une société privée pour installer une caméra vidéo qui enregistre les agissements sur le terrain du centre d'entretien, il s'agit d'un traitement de données sur mandat. C'est donc au mandant, à savoir à la commune, qu'incombe la responsabilité d'assurer la protection des données. La commune n'est cependant ni une autorité fédérale, ni une personne privée, c'est pourquoi elle n'est pas soumise à la LPD, mais aux dispositions de protection des données du canton concerné.

Le problème de vidéosurveillance par des organismes privés se présente selon notre point de vue de la manière suivante :
sont considérées comme données personnelles au sens de la LPD toutes les informations qui se rapportent à une personne identifiée ou identifiable. Est considéré comme traitement toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données. Si une caméra filme les usagers d'un point de collecte de déchets ménagers, les prises de vues révèlent des informations relatives à ces personnes. Il est

ainsi possible - sur la base du visage de la personne ou du numéro de plaque de sa voiture - d'identifier cette dernière. Le fait d'enregistrer les mouvements des personnes constitue une atteinte à la personnalité de ces dernières, ce qui peut être justifié pour prévenir ou pour punir des abus.
Même si l'enregistrement est justifié, les principes de base de la protection des données concernant le traitement tels que la proportionnalité et la finalité doivent être respectés. Cela signifie que ces enregistrements ne peuvent être faits et exploités que si le but recherché est de prévenir et de punir des abus. D'autres utilisations des enregistrements effectués ne seraient pas admissibles.
Le principe de la proportionnalité exige en outre que l'enregistrement se limite aux données vraiment nécessaires pour atteindre le but visé. Si les abus par exemple n'ont lieu que la nuit, les enregistrements ne doivent être faits que lors de courtes périodes nocturnes et non pendant la journée. D'autre part les enregistrements de mouvements qui visiblement ne constituent pas un abus doivent être immédiatement détruits.

9. Divers

9.1. Le registre du commerce comme banque électronique de données

Les nouvelles inscriptions dans le registre fédéral du commerce ont jusqu'à présent été publiées dans la Feuille officielle suisse du commerce (FOSC). L'Office fédéral du registre du commerce examine actuellement l'introduction de la gestion électronique du registre du commerce afin de simplifier l'accès au public des données qui y figurent.

L'Office fédéral du registre du commerce nous a demandé conseil au sujet de l'automatisation du registre du commerce. Le traitement des données des registres publics est réglé d'après des prescriptions très détaillées et formelles. Les dispositions du code des obligations (CO) et de l'ordonnance sur le registre du commerce (ORC) sont particulièrement importantes. Pour des raisons de sécurité du droit, ces prescriptions ne peuvent pas être modifiées par la LPD et par conséquent, le registre du commerce en tant que registre public de droit privé est exclu du champ d'application de la LPD. Cela n'exclut toutefois pas l'élaboration de dispositions particulières de protection des données dans le CO et l'ORC lors de nouveaux traitements de données. Dans ce contexte, on peut mettre en exergue les solutions prévues dans la LPD et l'OLPD ainsi que celles qui figurent dans la recommandation No R (91) 10 du Comité des ministres du Conseil de l'Europe aux Etats membres pour la transmission à des tiers des données personnelles enregistrées par les organes officiels.

Sur ces bases, nous avons conseillé dans une première étape de définir les catégories de données personnelles traitées ainsi que le but poursuivi par le traitement électronique. Il faudra par la suite désigner l'organe responsable du fichier, qui fixera les critères de sélection et de justification d'un besoin pour l'accès à ces données.
Bien que le registre présente un caractère public, cela n'implique pas que les données puissent être rendues accessibles et utilisées sans restriction. En effet, le principe de finalité est aussi applicable aux données accessibles au public. Cela

signifie que des données ne peuvent pas être transmises à des tiers si la communication n'est pas compatible avec le but pour lequel elles ont été collectées. Afin de permettre aux personnes concernées de se défendre contre un traitement de leurs données, il faut aussi garantir le droit d'accès. Dans l'intérêt de la sécurité des données, l'ensemble des critères susmentionnés doit être en accord avec les mesures techniques et organisationnelles.

9.2. Listes de participants à des voyages de groupes

Lors de l'organisation de voyages de groupes, les agences de voyage qui dressent et publient des listes d'adresses des participants devraient en informer au préalable les personnes concernées. Celui qui ne veut pas figurer sur la liste devrait pouvoir le signaler à l'agence de voyage, si possible lors de la conclusion du contrat.

Une entreprise de transport établissait depuis des années des listes d'adresses des participants à des voyages de groupes (composées du titre, des nom, prénom, adresse et nationalité). Le but de ces listes était d'informer mutuellement les participants avant le début du voyage afin d'organiser l'aller et le retour et de maintenir après le voyage les contacts établis. Suite à des réclamations, l'agence de voyage mit fin à cette pratique et s'adressa à nous afin de savoir si elle était autorisée à le faire.

En principe, il est permis d'utiliser des données personnelles pour dresser des listes si les personnes concernées en ont connaissance. L'établissement de listes de participants ne devient problématique que lorsque les personnes concernées n'en ont pas connaissance. Les données d'adresses sont en effet collectées par les agences de voyage pour le déroulement des relations contractuelles (réservation du voyage et facturation). Le traitement ultérieur des listes d'adresses qui sont communiquées à des tiers (autres participants au voyage) requiert par conséquent l'accord des personnes concernées. C'est pourquoi le client doit en être informé au préalable afin d'avoir la possibilité d'accepter ou de refuser le traitement ultérieur des données le concernant.

9.3. Formulaire de demande de location d'un véhicule

Dans le formulaire de demande de location d'un véhicule, il n'est pas admis de rédiger des clauses de consentement de manière si générale que le loueur peut chercher des renseignements auprès de n'importe qui. Le locataire doit voir de manière claire auprès de qui les informations qui lui sont demandées peuvent être recherchées et dans quel but il donne son consentement.

Un particulier nous a posé la question de savoir s'il était usuel que des renseignements soient recueillis auprès des PTT lors de la location d'une voiture. Il a résulté d'un examen du formulaire de demande qu'il fallait, outre le nom et l'adresse, indiquer la profession, l'employeur et son adresse ainsi que la durée de l'engagement. Simultanément, le loueur d'automobiles recevait l'autorisation de "pouvoir vérifier toutes les indications". Lorsqu'une clause de consentement est aussi générale, le client ne peut pas vérifier auprès de quels organes ou organisations d'autres recherches sont entreprises à son sujet. Du point de vue du droit de la

protection des données, une telle autorisation n'est pas valable, vu que le locataire ne peut donner son accord que pour un objet clairement déterminé.

Suite à cette prise de position, l'entreprise concernée a révisé son formulaire de manière conforme à la protection des données et la clause de consentement a la nouvelle teneur suivante : "Le locataire autorise le loueur à vérifier ces indications auprès de l'employeur ou de l'adresse de référence indiquée."

9.4. Demande de consultation de dossiers de hauts fonctionnaires de la part du Dictionnaire historique de la Suisse auprès des Archives fédérales

Le Dictionnaire historique de la Suisse (DHS) désire rédiger des articles biographiques d'une longueur de dix lignes sur certains hauts fonctionnaires. Afin de se procurer les informations nécessaires concernant les hauts fonctionnaires qui ne sont plus en fonction, le DHS s'est adressé aux Archives fédérales (AF) en leur demandant de pouvoir consulter les dossiers personnels des fonctionnaires concernés en possession des AF. Pour des raisons de protection des données, nous n'avons pas pu approuver l'octroi d'une consultation générale de ces dossiers.

Une partie des fonctionnaires concernés sont encore vivants, d'autres déjà décédés. La question qui se pose est de savoir s'il est admissible de rendre des dossiers personnels contenant des données sensibles ou des profils de la personnalité accessibles à des tiers, afin de leur permettre de publier un article biographique d'environ 10 lignes au sujet de la personne concernée. La communication de données personnelles par les AF est actuellement encore régie par un règlement interne. Les dispositions de ce dernier doivent néanmoins être interprétées conformément à la protection des données.
Selon le règlement, les données personnelles peuvent être rendues accessibles au public sans restrictions après un délai de 35 ans, pour autant que cette publication ne porte pas préjudice à un intérêt public ou privé. Cela signifie qu'il est nécessaire de vérifier dans chaque cas d'espèce, si la consultation d'un dossier déposé aux AF porte atteinte à des intérêts privés. Il importe également de peser le pour et le contre des divers intérêts en présence.
Les dossiers du service du personnel contiennent en règle générale des données sensibles (telles que dossiers et certificats médicaux). Il est également possible que les données contenues dans le dossier du service du personnel (telles que qualifications, entretiens d'appréciation, curriculum vitae, informations relatives à la situation familiale) permettent de constituer un profil de la personnalité de la personne concernée. Si cette personne est encore en vie, on doit partir du principe qu'un tel droit de consultation peut porter préjudice à ses intérêts privés. C'est pourquoi de telles données personnelles ne doivent pas être mises à disposition du public, même après 35 ans, sauf si la personne concernée donne son consentement.

Une consultation de dossiers du service du personnel de personnes décédées ne peut être autorisée que si le requérant justifie un intérêt à la consultation et si cette dernière ne porte pas préjudice à des intérêts prépondérants de tiers ou de proches de la personne décédée.
Dans le cas présent, la consultation - que ce soit pour les personnes vivantes ou décédées - ne peut pas être autorisée pour des raisons de proportionnalité. Il est excessif de mettre à disposition de tier des documents contenant des données

sensibles ou permettant d'établir des profils de la personnalité, si le seul but poursuivi consiste à collecter des informations permettant de rédiger un article biographique d'une longueur de dix lignes.

9.5. Enregistrement d'interviews scientifiques

La Phonothèque nationale Suisse conduit en collaboration avec l'Office fédéral de la communication des interviews scientifiques avec des témoins historiques au sujet du rôle de la Suisse dès les années 30. Les enregistrements de ces interviews devraient ensuite être répertoriés dans une banque de données et mis à disposition de la recherche scientifique.

La Phonothèque nationale Suisse, en collaboration avec l'Office fédéral de la communication, conduit une série d'interviews scientifiques avec des témoins historiques au sujet du rôle de la radio en Suisse à partir des années 30. Ceci concerne d'une part des pionniers de la radio, mais également des auditeurs de cette époque. Il est prévu de stocker ces enregistrements dans une banque de données et de les rendre accessibles à la recherche scientifique.

La Phonothèque nationale Suisse nous a contactés car elle tient à ce que ce projet scientifique soit en tous points conforme aux dispositions légales. C'est la raison pour laquelle elle nous a fait parvenir le projet d'un règlement relatif à la saisie des données, ainsi qu'au traitement et à l'utilisation ultérieurs des données par des tiers.

Nous avons émis l'avis selon lequel le règlement doit en principe être accessible à toutes les personnes interrogées avant leur l'interview et tous les documents ou copies ne doivent être accessibles au public que sous forme anonyme, à part quelques exceptions devant être régies séparément. Nous avons d'autre part rendu la Phonothèque nationale Suisse attentive au fait que c'est elle, en qualité de maître du fichier, qui est responsable d'assurer la protection des données. Nous avons d'ailleurs pu approuver le projet de règlement qui nous a été soumis. Nos exigences ont été entièrement prises en compte.

9.6. Adoptions et recherches du lieu de séjour

Les recherches sur les parents biologiques sont de plus en plus souvent effectuées par des organes de médiation privés. Dans ce contexte, on demande fréquemment des adresses aux autorités. C'est bien sûr la tâche des autorités d'adoption compétentes, après avoir procédé aux éclaircissements nécessaires et pondéré les intérêts en présence, de communiquer aux personnes qui le demandent l'adresse des parents biologiques à condition que ces derniers soient d'accord.

Différentes institutions de médiation pour les enfants adoptifs ont demandé au contrôle de l'habitant d'une commune les adresses des parents naturels. Contrairement aux organes officiels, les offices de médiation n'ont pas l'obligation de détruire les dossiers d'adoption après l'adoption et ont ainsi la possibilité de rechercher l'adresse actuelle des parents biologiques sur la base de leur ancien domicile. Le contrôle de l'habitant s'est adressé à nous pour savoir dans quelle mesure la réponse à de telles questions était conciliable avec le secret de l'adoption.

Les contrôles de l'habitant sont des organes communaux soumis aux prescriptions cantonales de protection des données. En l'absence de prescriptions cantonales, le traitement de données personnelles par des organes cantonaux en application du droit fédéral est soumis à certaines dispositions de la LPD. Dans le cas présent, en tant qu'organes cantonaux, les offices de contrôle de l'habitant appliquent le droit fédéral, raison pour laquelle certaines dispositions de la LPD sont appliquées dans les cantons sans loi cantonale sur la protection des données. Ces cantons déterminent un organe de contrôle qui veille au respect de la protection des données.

Comme la connaissance de l'ascendance constitue un élément important pour le développement personnel de l'être humain, la question se pose de savoir qui doit être protégé par le secret de l'adoption. Il s'agit en premier lieu de l'enfant. Les parents biologiques d'un enfant ne devraient pas avoir la possibilité, par des contacts ultérieurs avec lui, de se mêler de son éducation et de mettre ainsi en péril la réussite de l'adoption. La famille formée par l'adoption doit pouvoir se développer sans influence extérieure à l'instar d'une famille constituée par descendance naturelle. Pour cette raison, l'identité des parents adoptifs ne peut pas être communiquée sans leur accord aux parents naturels. L'intégration sociale de l'enfant dans sa nouvelle famille en tant qu'objectif principal visé par le secret de l'adoption n'exige toutefois pas que l'obligation du maintien du secret se justifie à jamais.

Lorsque l'enfant exprime le désir de connaître ses parents naturels, nous sommes d'avis qu'il faut procéder à une pesée des intérêts. C'est aux autorités d'adoption, et non aux organes privés de médiation, d'examiner s'il existe effectivement un intérêt prépondérant de la personne concernée à ce qu'on lui communique les données et dans quelle mesure les autres participants (parents adoptifs et parents naturels) sont prêts à cette indication d'identité ou si d'autres intérêts plausibles s'y opposent. La responsabilité de la prise de décision incombe toujours de cas en cas et librement à l'autorité compétente.

9.7. Groupe de travail des cantons

La collaboration avec les autorités cantonales de protection des données fait partie des tâches légales du Préposé fédéral à la protection des données. Elle revêt une grande importance notamment eu égard aux nombreux traitements et systèmes d'informations Confédération-cantons. Cette collaboration intervient notamment par le biais de la Conférence suisse des commissaires à la protection des données (voir p. 197) et par notre participation à un groupe de travail mis en place par les préposés cantonaux de Zurich, Berne, Bâle-campagne, Fribourg et Lucerne.

Ce groupe de travail informel a pour objectif de renforcer les échanges d'informations entre les cantons sur des questions communes. Ce groupe de travail est ouvert à toutes les autorités cantonales de protection des données qui le souhaitent et qui sont prêtes à y apporter une collaboration active. Le groupe de travail souhaite également renforcer la collaboration avec le préposé fédéral et l'a invité à ses réunions. Nous avons accepté d'y prendre part en fonction des thèmes abordés, et dans la mesure où cette participation ne se fait pas au détriment des autres cantons et de la Conférence suisse des commissaires à la protection des données. Nous avons ainsi participé à trois réunions, l'une consacrée à l'information

cantons-Confédération, l'autre à la sécurité des données sur les réseaux et la troisième aux données concernant la santé.

IV. ACTIVITES INTERNATIONALES

1. Conférence Internationale des Commissaires à la protection des données

La XVIIe Conférence Internationale des Commissaires à la protection des données s'est déroulée à Copenhague du 6 au 8 septembre 1995, à l'invitation du commissaire danois. La Conférence réunissait les commissaires à la protection des données de 25 Etats, des experts gouvernementaux, des représentants de l'Union européenne et de l'économie, de la science et des services. La Suisse y était représentée par le préposé fédéral suppléant et par le préposé du canton de Zurich. La Conférence a permis de faire le point sur les développements internationaux récents et en particulier la directive européenne relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation des données. Elle a également permis un échange approfondi sur la protection de la vie privée dans le domaine de l'emploi (problème de la surveillance automatisée sur les lieux de travail : surveillance de l'acte professionnel et notamment suivi automatique du temps de travail, enregistrement des conversations téléphoniques en particulier aux fins de contrôle de l'efficacité du travail et de sa qualité, surveillance des réseaux, vidéosurveillance et émergence du contremaître électronique; utilisation des données génétiques aux fins d'emploi; information des personnes concernées sur leurs droits). La Conférence a en outre abordé les problèmes de protection des données dans les secteurs de la recherche et de la statistique, en particulier à la lumière des exemples des pays nordiques et des travaux du Conseil de l'Europe. Elle s'est ensuite penchée sur les développements technologiques qui engendrent de nouveaux risques pour la vie privée et la protection des données (en particulier multiplication des traces électroniques sans que la personne concernée puisse avoir une vue globale ou un suivi de toutes les liaisons individuelles qu'elle établit, multifonctionnalité et multimédias, numérisation, traitement des images et de la voix). Aux yeux des commissaires à la protection des données, il est urgent de renforcer la protection et la sécurité des données face à ces nouvelles technologies. En effet, ces dernières bouleversent profondément la manière de traiter les données, en combinant notamment son, image et texte et en permettant une grande diffusion de l'information et des combinaisons infinies. Il est en particulier nécessaire de restreindre l'utilisation de données personnelles, en recourant notamment à des procédures anonymes (paiement anonyme, liaison anonyme, etc.) et en limitant l'accès aux données en fonction des finalités poursuivies. Les procédures de contrôle doivent être améliorées, notamment en développant et en recourant à des logiciels spécifiques à la protection des données. Il est également indispensable d'introduire des technologies de la vie privée dans la conception et le développement des systèmes d'information (technique de chiffrement, technologie garantissant l'anonymat, notamment par utilisation de pseudo-identité à utilisation unique). Enfin les commissaires ont réaffirmé l'importance de l'information du public pour sensibiliser les différents acteurs aux

risques des nouvelles technologies, les rendre plus vigilants et encourager les individus à exercer leurs droits.

2. Conseil de l'Europe

Sous présidence suisse, le Groupe de projet sur la protection des données du Conseil de l'Europe s'est réuni à deux reprises. Il a en particulier poursuivi ses travaux en vue de l'adoption d'une recommandation relative à la protection des données médicales et d'une recommandation relative à la protection des données à caractère personnel collectées et traitées à des fins statistiques. Ces deux instruments devraient être finalisés cette année et adoptés par le Comité des Ministres dans le courant 1997. En outre, nous avons participé aux travaux du groupe de travail 14, chargé de préparer un projet de recommandation relative à la protection des données personnelles à des fins d'assurances privées. Enfin, un nouveau groupe de travail a entamé ses travaux dans le domaine des nouvelles technologies de l'information, notamment les autoroutes de l'information (Internet) et les multimédias.

Pour sa part, le Comité consultatif mis en place par la Convention 108 et qui est chargé en particulier de donner des avis sur l'application de ladite Convention a poursuivi ses travaux sur la définition de données à caractère personnel, notamment pour la voix et l'image, ainsi que sur la notion d'"enfant à naître". Il a émis un avis sur la "compatibilité des données" et admis que dans la mesure où certaines garanties sont aménagées, l'utilisation à des fins statistiques de données personnelles collectées à d'autres fins est en principe compatible avec le but initial du traitement. Il a écarté une proposition d'un Etat contractant d'élaborer un protocole additionnel à la Convention 108 tendant à renforcer l'assistance internationale aux personnes concernées. Enfin à notre demande, il a émis un avis sur les conditions de ratification de la Convention 108, dans lequel il relève en particulier que notre pays répond aux critères exigés par la Convention en vue de sa ratification. Ainsi, malgré le fait que certains cantons n'ont pas encore de loi de protection des données, le droit suisse offre des garanties suffisantes et conformes aux exigences de la Convention permettant ainsi à la Suisse de la ratifier.

La Convention européenne pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) est un pas important vers l'harmonisation des législations nationales et pour le développement de la coopération internationale. De la sorte, un niveau élevé de protection des données peut être assuré, tout en garantissant la libre circulation des informations. Elle s'applique à tous les fichiers et traitements automatisés de données personnelles dans les secteurs public et privé, dans la mesure où ces données concernent des personnes physiques identifiées ou identifiables. Elle définit les principes et bases de la protection des données que les Etats parties doivent concrétiser dans leur ordre juridique interne. Elle exclut en principe les entraves aux flux transfrontières de données entre les Etats parties. Elle règle la coopération entre Etats pour la mise en oeuvre de la Convention et en particulier l'assistance qu'un Etat contractant doit porter aux personnes concernées ayant leur résidence à l'étranger. Cette Convention a été ratifiée par 17 Etats membres. Quatre autres l'ont signée. A l'exception de la Suisse et de la Hongrie, tous les Etats qui n'ont pas encore ratifié la

Convention ne jouissent pas encore de législation conforme aux exigences de ladite Convention.

Sur mandat du DFJP, nous avons poursuivi les travaux en vue de la ratification de la Convention 108. Le Conseil fédéral devrait adopter son message au Parlement durant l'été, rendant une ratification possible dans la première moitié de la présente législature. La ratification de cette Convention répond à une nécessité politique et juridique dans un monde de plus en plus interactif. Elle permettra finalement de renforcer la protection juridique des individus lors du traitement de données personnelles tout en facilitant l'échange d'informations entre la Suisse et les autres Etats parties.

3. Union européenne

La directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard des données à caractère personnel et à la libre circulation de ces données a été adoptée le 24 octobre 1995. Les Etats membres de l'Union européenne et de l'Espace Economique Européen ont trois ans pour transposer la directive dans leur droit national.
L'objectif de cette directive européenne est d'assurer un haut niveau de protection de la vie privée des citoyens dans tous les Etats membres, tout en permettant la libre circulation des données personnelles à l'intérieur de l'Union européenne et de l'Espace Economique Européen. Elle vise également à supprimer les distorsions de concurrence et les risques de délocalisation. La directive couvre le traitement de données personnelles dans les secteurs public et privé dans la mesure où ces traitements entrent dans le champ de compétence de l'Union européenne. La directive ne s'applique ainsi pas aux traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'Etat. Elle ne fait aucune distinction entre secteurs public et privé. La directive stipule les conditions dans lesquelles un traitement automatisé ou non automatisé de données personnelles est légitime. Elle énonce les droits de la personne concernée (en particulier droit à l'information, droit d'accès, droit de rectification, droit de s'opposer au traitement, recours). Elle règle les qualités que doivent avoir les données personnelles (notamment exactitude, collecte loyale et licite, finalité légitime et licite, compatibilité, proportionnalité), la confidentialité et la sécurité des traitements, la notification des traitements et la surveillance (autorité de contrôle indépendante avec pouvoir de décision et droit d'ester en justice). La directive abandonne la référence au fichier, sauf pour les données manuelles, pour se concentrer sur les traitements. Enfin, elle règle les flux transfrontières de données. Ceux-ci doivent être libres au sein de l'Union européenne. Ils sont par contre en principe interdits vers des Etats tiers, dans la mesure où ceux-ci ne jouissent pas d'une législation de protection des données jugée adéquate. La directive a également pour ambition de préciser et amplifier les principes de la Convention no 108 du Conseil de l'Europe. Nous avons élaboré à l'intention du chef du DFJP un premier rapport sur les conséquences de la directive pour la Suisse. Nous sommes ainsi parvenus à la conclusion que la loi fédérale sur la protection des données n'était pas en tous points conforme à la directive européenne. Toutefois, notre législation, conforme aux exigences de la Convention 108, offre un niveau de protection suffisant et adéquat eu égard aux exigences de la directive. Une modification de la loi ne s'avère actuellement pas nécessaire. On ne peut cependant pas exclure la nécessité d'une modification ultérieure pour rendre

notre droit eurocompatible. Il convient néanmoins d'attendre la transposition par les Etats membres de la directive dans leur droit interne avant d'envisager une telle modification. Les principales lacunes concernent les conditions du consentement, les exigences au niveau de la finalité, le traitement des données sensibles, le droit à l'information des personnes concernées, l'étendue du droit d'accès, les décisions individuelles automatisées, la responsabilité civile, la notification des traitements (dans le secteur privé en particulier) et le pouvoir de décision de l'autorité de contrôle indépendante.

V. REGISTRE DES FICHIERS

1. Bilan

Malgré les difficultés évoquées dans nos deux premiers rapports (p. 158 et 182), les travaux de contrôle et d'enregistrement suivent leur cours. Une publication partielle du registre des fichiers dans la Feuille fédérale est prévue prochainement.

Les travaux de contrôle et d'enregistrement des annonces de fichiers et de flux transfrontières se poursuivent. La publication d'une partie des fichiers du secteur public, ainsi que de l'intégralité des fichiers du secteur privé qui nous ont été annoncés, est prévue pour cet été.

2. DATAREG - Système de gestion du registre des fichiers

En service depuis un peu plus d'un an maintenant, le système de gestion du registre des fichiers a été optimalisé d'après les expériences déjà rassemblées. A partir des saisies effectuées, il est désormais possible de tirer les premières conclusions sur l'impact et les propriétés des entrées.

Alors que l'année 1994 a été placée sous le signe de la mise en service officielle de DATAREG, 1995 a été l'année des premières expériences; elles ont été exploitées et l'ensemble du système a été optimalisé. Nous avons par exemple reçu des suggestions de la part des maîtres de fichiers, les feuilles de contrôle ont été restructurées et leur présentation remaniée, de nouveaux champs ont été ouverts, les longueurs ont été adaptées et l'espace réservé aux utilisateurs a été amélioré.

Les considérations et chiffres ci-dessous relatifs aux fichiers enregistrés se rapportent à l'état du registre en janvier 1996.

710 fichiers au total ont été enregistrés. 18 de ces entrées ont été déjà effacées sur demande du maître du fichier. 605 entrées proviennent d'organes fédéraux et 87 de particuliers. Sur les 692 fichiers enregistrés, tous sont soumis à publication à l'exception de quatre d'entre eux.

Sur les formulaires de déclaration, 17 catégories de données personnelles traitées figurent à choix et à titre d'exemples. Toutefois 685 catégories différentes de données personnelles ont été jusqu'ici saisies dans le registre. Ces catégories ont

été utilisées par les entrées 5187 fois. Les catégories de données personnelles les plus souvent mentionnées sont l'adresse, la profession, la nationalité/le lieu d'origine, avant l'identité et le numéro AVS.

567 catégories de destinataires de données et de participants ont été enregistrées; elles ont été citées 1578 fois comme destinataires et 389 fois comme participants.

En ce qui concerne les déclarations faites par les organes fédéraux, 286 bases légales différentes ont été jusqu'ici mentionnées. Elles ont été utilisées 880 fois.

666 adresses de maîtres de fichiers ont été jusqu'ici intégrées dans le système. 16 catégories de branches ont été attribuées pour la saisie de fichiers privés.

VI. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

1. Déplacement du siège du PFPD du centre de la ville de Berne à Zollikofen

Le siège du PFPD et de son Secrétariat se trouve à la Monbijoustrasse 5, au centre de la ville de Berne, depuis mars 1993. Or, le 2 avril 1996, le Département fédéral de justice et police a décidé que le siège du PFPD devait nouvellement se trouver à Zollikofen, situé à 25 minutes du centre (si l'on recourt aux transports publics). Suite à cette décision, l'accomplissement des tâches légales du PFPD va être considérablement entravé.

C'est d'ailleurs en raison du caractère particulier desdites tâches, que le Conseil fédéral avait expressément fixé le siège du PFPD en ville de Berne, et ce dans l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (article 30, 1er alinéa). En effet, le PFPD doit être régulièrement en contact tant avec les organes fédéraux qu'avec les personnes privées (maîtres de fichiers et personnes concernées), par le biais de séances, contrôles, inspections oculaires, séminaires, conférences etc. Ces tâches requièrent une mobilité de l'ensemble du Secrétariat du PFPD qu'il ne faut pas sous-estimer.

Le Département fédéral de justice et police s'est déjà trouvé confronté à la décision du déplacement du PFPD hors de la ville de Berne, et ce avant l'entrée en vigueur de la LPD. A cette période, il avait reconnu la nécessité d'une localisation centralisée - tant interne à l'administration que pour toute la Suisse - et avait revu sa décision relative au déménagement du PFPD à Zollikofen en faveur de son installation à la Monbijoustrasse.

La décision du Département fédéral de justice et police du 2 avril 1996 semble sans appel. Or, la délocalisation du PFPD et de son Secrétariat générera des pertes considérables en temps de travail pour ses collaborateurs. Les personnes privées et les organes fédéraux désireux de recourir aux conseils du PFPD, respectivement à une consultation, seront également désavantagés. Outre l'accroissement des coûts de déplacement, des coûts administratifs supplémentaires découleront des pertes de temps inévitables en l'espèce.

2. Evolution des tâches

Nous avons constaté cette année un accroissement du volume des tâches dans les domaines des télécommunications, de la santé et du personnel. La vérification de fichiers déclarés et le développement du registre des fichiers ont occupé une part considérable des capacités de nos services. D'autre part, nous avons été davantage consultés par la population, notamment sur les problèmes de surveillance au poste de travail et d'utilisation des nouvelles technologies de communication, sur les agences de renseignements économiques et sur les questions de marketing direct, pour ne citer que quelques domaines.

3. Information du public

Au cours de l'exercice écoulé également, le PFPD et ses collaborateurs ont présenté des exposés sur des questions de protection des données à l'occasion de diverses manifestations d'information, conférences et colloques.

Par ailleurs, nous avons informé le public par communiqués de presse du fichier des journalistes de Zermatt, des problèmes de protection des données que pose INTERNET, et de la deuxième conférence suisse des commissaires à la protection des données. Cette année également, nous avons envoyé un nombre considérable de brochures à des particuliers et à des autorités.


Service téléphonique du PFPD

Outre les questions qui nous sont parvenues par écrit (cf. à ce propos tableaux p. 200, 201), nous avons aussi répondu à un nombre considérable de questions par téléphone.
Les tableaux des pages 202, 203, 204 présentent par thèmes les diverses questions qui nous ont été posées.

4. Deuxième Conférence suisse des commissaires à la protection des données 1995

La conférence a traité des questions actuelles de protection des données, qui occupent les autorités de protection des données aussi bien au niveau cantonal que fédéral. Ce fut également une occasion bienvenue d'échanger les expériences faites.

Le 20 octobre 1995 eut lieu à Berne la deuxième conférence suisse des commissaires à la protection des données organisée par le PFPD avec la participation active de représentantes et représentants des organes de protection des données des cantons.

Les sujets suivants ont principalement été traités : le droit d'accès dans le domaine de la santé publique, les avantages et inconvénients d'un numéro personnel

d'identification, l'accès des cantons aux applications fédérales, la sécurité informatique Confédération-cantons, le recensement de la population de l'an 2000, l'amélioration de l'échange d'informations entre les organes cantonaux de protection des données et le PFPD, l'activité de la Commission fédérale de la protection des données ainsi que la communication de l'identité des détenteurs de véhicules motorisés par l'intermédiaire du numéro 111 et de Swiss Online (vidéotex). Une résolution a été prise à ce sujet demandant à ce qu'un détenteur de véhicule ait le droit d'interdire la publication et la communication de son identité, sans qu'il doive justifier d'un intérêt particulier.

Sur la base des expériences positives qui ont été faites, il est prévu que la Conférence des commissaires à la protection des données ait dorénavant lieu tous les ans. Le préposé à la protection des données du canton de Zurich s'est déclaré prêt à assumer l'organisation de celle-ci pour l'année 1996.

5. Statistique des activités du Préposé fédéral à la protection des données

Période du 1er avril 1995 au 31 mars 1996

Participations à des conférences:

Nationales	Internationales
25	15

Nombre de séances:

	Confédération	Personnes privées	Cantons
A l'intérieur	101	35	1
A l'extérieur	194	22	1
Total	295	57	2

Nombres de prises de position

Nombres de prises de position

Renseignements par telephone

Renseignements par telephone
Selon la provenance des appels

Renseignements par telephone
Par matière

6. Composition du Secrétariat du Préposé fédéral à la protection des données

Préposé fédéral à la protection des données :	**Guntern Odilo, dr en droit**
Suppléant :	Walter Jean-Philippe, dr en droit
Secrétariat :	
Chef :	Walter Jean-Philippe, dr en droit
Suppléant :	Buntschu Marc, lic. en droit
Délégué Presse et Information :	Tsiraktsopulos Kosmas, lic. en droit
Service juridique :	9 personnnes
Service informatique :	3 personnes
Chancellerie :	4 personnes

VII. ANNEXES

CONSEIL DE L'EUROPE

COMITE DES MINISTRES

RECOMMANDATION N° R (95) 4

DU COMITE DES MINISTRES AUX ETATS MEMBRES

SUR LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL DANS LE DOMAINE DES SERVICES DE TÉLÉCOMMUNICATION, EU ÉGARD NOTAMMENT AUX SERVICES TÉLÉPHONIQUES

(adoptée par le Comité des Ministres le 7 février 1995, lors de la 528e réunion des Délégués des Ministres)

Le Comité des Ministres, en vertu de l'article 15.b du Statut du Conseil de l'Europe,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Conscient de l'utilisation croissante de l'informatique dans le domaine des services de télécommunication et des avantages que les utilisateurs retirent des développements technologiques, en particulier dans le domaine des services téléphoniques;

Ayant à l'esprit, dans ce contexte, l'évolution vers la numérisation des réseaux ainsi que les avantages que celle-ci entraîne pour les utilisateurs des services de télécommunication;

Estimant, toutefois, que le développement technologique dans le domaine des télécommunications, en particulier des services téléphoniques, peut comporter des risques éventuels pour la vie privée de l'utilisateur ainsi que d'éventuelles entraves à sa liberté de communication;

Se référant à cet égard à certaines nouvelles caractéristiques notamment dans le domaine des services téléphoniques, par exemple l'identification de la ligne d'appel, le service de transfert d'appel et les téléphones mobiles, ainsi que les dispositifs de recherche des appels malveillants et les automates d'appel;

Notant également les risques pour la vie privée et la liberté de communication liés à l'obtention de factures téléphoniques détaillant les numéros appelés;

Reconnaissant que les dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Strasbourg 1981, STE 108) s'appliquent aux activités de traitement automatisé des données par

des exploitants de réseau et toute autre personne fournissant des services de télécommunication;

Estimant néanmoins qu'il convient de préciser les dispositions générales de la convention pour les adapter à la collecte et au traitement des données à caractère personnel par les exploitants de réseau et toute autre personne fournissant des services de télécommunication;

Notant, en outre, que les nouveaux développements intervenus dans les services de télécommunication sont soumis au respect du droit à la vie privée et au secret de la correspondance tels que garantis par l'article 8 de la Convention européenne des Droits de l'Homme,

Recommande aux gouvernements des Etats membres :

- de tenir compte, dans leurs droit et pratique internes, des principes énoncés dans l'annexe à la présente recommandation;

- de porter la présente recommandation à l'attention de toute autorité participant à la mise en œuvre d'une politique nationale de protection des données ou de télécommunication;

- de s'assurer que les dispositions de la recommandation sont portées à l'attention des exploitants de réseau, des fournisseurs de services de télécommunication, des fabricants d'équipement matériel et logiciel, des organismes utilisant les télécommunications à des fins de marketing direct, ainsi que des organes les représentant et des organisations de consommateurs;

- de promouvoir les dispositions de la recommandation au sein des divers organes internationaux traitant de télécommunication.

Annexe à la recommandation n° R (95) 4

1. *Champ d'application et définitions*

1.1. Les principes énoncés dans la présente recommandation s'appliquent aux exploitants de réseau et aux fournisseurs de services qui, dans l'accomplissement de leurs fonctions, collectent et traitent des données à caractère personnel.

1.2. Ces principes s'appliquent aux données à caractère personnel qui font l'objet d'un traitement automatisé.

Les Etats membres peuvent étendre les principes énoncés dans la présente recommandation aux données à caractère personnel qui font l'objet d'un traitement manuel.

1.3. Les Etats membres peuvent étendre les principes énoncés dans la présente recommandation à la collecte et au traitement des données à caractère personnel relatives aux personnes morales.

1.4. Aux fins de la présente recommandation :

- l'expression «données à caractère personnel» signifie toute information concernant une personne identifiée ou identifiable (personne concernée). Une personne physique n'est pas considérée comme «identifiable» si cette identification nécessite des délais ou des activités déraisonnables;

- l'expression «services de télécommunication» recouvre les diverses prestations offertes par l'entremise des réseaux de télécommunication permettant aux utilisateurs de communiquer entre eux ou de correspondre par message vocal, texte, image ou par transmission de données;

- l'expression «exploitants de réseau» recouvre toute entité publique ou privée qui rend disponible l'utilisation d'un réseau de télécommunication;

- l'expression «fournisseurs de services» recouvre toute entité publique ou privée qui fournit et gère des services de télécommunication en utilisant soit un réseau mis à disposition par un exploitant de réseau, soit son propre réseau.

2. *Respect de la vie privée*

2.1. Les services de télécommunication, et en particulier les services téléphoniques en cours de développement, devraient être offerts dans le respect de la vie privée des utilisateurs, du secret de la correspondance et de la liberté de communication.

2.2. Les exploitants de réseau et les fournisseurs de services et d'équipement matériel et logiciel devraient tirer parti de la technologie de l'information pour fabriquer et exploiter des réseaux, des équipements et des logiciels respectant la vie privée des utilisateurs.

Des dispositifs anonymes d'accès au réseau et aux services de télécommunication devraient être mis à disposition.

2.3. A moins que cela ne soit autorisé pour des raisons techniques d'enregistrement ou de transmission de messages, pour d'autres raisons légitimes ou pour l'exécution d'un contrat de services passé avec l'abonné, toute ingérence dans le contenu de la communication soit par les exploitants de réseau, soit par les fournisseurs de services devrait être interdite. Sous réserve du principe 4.2, les données relatives au contenu des messages collectées lors d'une telle ingérence ne devraient pas être communiquées à des tiers.

2.4. Il ne peut y avoir ingérence des autorités publiques dans le contenu d'une communication, y compris l'utilisation de tables d'écoute ou d'autres moyens de surveillance ou d'interception des communications, que si cette ingérence est

prévue par la loi et constitue une mesure nécessaire, dans une société démocratique :

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

2.5. En cas d'ingérence des autorités publiques dans le contenu d'une communication, le droit interne devrait réglementer :

a. l'exercice des droits d'accès et de rectification par la personne concernée;

b. les conditions dans lesquelles les autorités publiques compétentes seront en droit de refuser de donner des renseignements à la personne concernée ou d'en différer la délivrance;

c. la conservation ou la destruction de ces données.

Lorsqu'un exploitant de réseau ou un fournisseur de services est chargé par une autorité publique d'effectuer une ingérence, les données ainsi collectées ne devraient être communiquées qu'à l'organisme désigné dans l'autorisation pour cette ingérence.

2.6. Le droit interne devrait déterminer les conditions et les garanties en vertu desquelles les exploitants de réseau sont autorisés à utiliser des moyens techniques pour localiser l'origine des appels malveillants ou abusifs.

3. *Collecte et traitement des données*

3.1. La collecte et le traitement des données à caractère personnel dans le domaine des télécommunications devraient être effectués et développés dans le cadre d'une politique de protection des données, en tenant compte des dispositions énoncées dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, et notamment du principe de finalité.

Sans préjudice d'autres finalités prévues dans la présente recommandation, les données à caractère personnel ne devraient être collectées et traitées par les exploitants de réseau et les fournisseurs de services qu'aux fins de raccordement au réseau et de mise à disposition d'un service de télécommunication déterminé, et aux fins de facturation et de vérification du paiement, ainsi que pour assurer la mise en œuvre technique optimale et le développement du réseau et du service.

3.2. Les exploitants de réseau et les fournisseurs de services devraient informer de manière appropriée les abonnés aux services de télécommunication des catégories de données à caractère personnel collectées et traitées les concernant, du fondement juridique de la collecte, des finalités pour lesquelles elles sont collectées et traitées, de l'utilisation qui en est faite et des durées de conservation.

4. *Communication des données*

4.1. Les données à caractère personnel collectées et traitées par les exploitants de réseau ou les fournisseurs de services ne devraient pas être communiquées, à moins que l'abonné concerné n'ait donné par écrit son consentement exprès et éclairé et que l'information communiquée ne permette pas d'identifier les abonnés appelés.

L'abonné peut retirer son consentement à tout moment mais de manière non rétroactive.

4.2. Les données à caractère personnel collectées et traitées par les exploitants de réseau ou les fournisseurs de services peuvent être communiquées aux autorités publiques si cette communication est prévue par la loi et constitue une mesure nécessaire, dans une société démocratique :

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

4.3. En cas de communication de données à caractère personnel à des autorités publiques, le droit interne devrait réglementer :

a. l'exercice des droits d'accès et de rectification par la personne concernée;

b. les conditions dans lesquelles les autorités publiques compétentes seront en droit de refuser de donner des renseignements à la personne concernée ou d'en différer la délivrance;

c. la conservation ou la destruction de ces données.

4.4. Les listes d'abonnés qui contiennent des données à caractère personnel ne peuvent être communiquées par des exploitants de réseau et des fournisseurs de services à des tiers que si l'une des conditions suivantes est remplie :

a. l'abonné a donné par écrit son consentement exprès et éclairé, ou

b. l'abonné, informé de la communication envisagée, n'a pas formulé d'objection, ou

c. l'autorité chargée de la protection des données a autorisé la communication, ou

d. la communication est prévue par le droit interne.

L'abonné peut retirer son consentement à tout moment mais de manière non rétroactive.

4.5. La communication de données à caractère personnel entre exploitants de réseau et fournisseurs de services est permise lorsque cette communication est nécessaire à des fins opérationnelles et de facturation.

5. *Droits d'accès et de rectification*

5.1. Chaque abonné devrait pouvoir, sur demande et à des intervalles raisonnables, et sans délai ou frais excessifs, obtenir toutes les données le concernant collectées et traitées par les exploitants de réseau ou par les fournisseurs de services, et les faire rectifier ou effacer lorsqu'elles sont inexactes, non pertinentes ou excessives, ou lorsqu'elles ont été conservées pendant une durée excessive.

5.2. La satisfaction des demandes formulées en vertu du principe 5.1 peut être refusée, restreinte ou différée si la loi le permet et si cela constitue une mesure nécessaire, dans une société démocratique :

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;

b. à la protection de la personne concernée et des droits et libertés d'autrui.

6. *Sécurité*

6.1. Les exploitants de réseau et les fournisseurs de services devraient prendre toutes les mesures techniques et organisationnelles appropriées pour assurer la sécurité physique et logique du réseau, des services et des données qu'ils collectent et traitent, et empêcher toute ingérence ou interception non autorisée des communications.

6.2. Les abonnés aux services de télécommunication devraient être informés des risques de violation de la sécurité des réseaux, et de la manière dont ils peuvent limiter les risques de sécurité de leurs messages.

7. *Application des principes*

a. Annuaires

7.1. Les abonnés devraient avoir le droit de refuser, à titre gratuit et sans motivation, que leurs données à caractère personnel figurent dans un annuaire.

Toutefois, lorsque le droit interne exige que certaines données soient incluses dans un annuaire, l'abonné devrait pouvoir faire exclure ses données sur justificatif.

Lorsque le droit interne exige d'un abonné un paiement afin que ses données ne soient pas incluses dans un annuaire, ce paiement devrait être d'un montant raisonnable et ne devrait, en aucun cas, être dissuasif pour l'exercice de ce droit.

7.2. Lorsqu'un abonné demande l'inscription de co-utilisateurs de son terminal dans un annuaire, il devrait au préalable avoir recueilli leur consentement.

7.3. Sous réserve du cas où l'abonné souhaite inclure des données supplémentaires le concernant, les données à caractère personnel contenues dans un annuaire

devraient être limitées aux données nécessaires à identifier raisonnablement un abonné particulier et à empêcher une confusion entre ou parmi différents abonnés figurant dans l'annuaire.

7.4. Lors de la consultation d'un annuaire électronique, des moyens techniques devraient être mis en place pour prévenir les abus et notamment les télédéchargements non autorisés.

L'appariement de données contenues dans un annuaire électronique avec d'autres données ou d'autres fichiers devrait être interdit, sauf si le droit interne le permet ou si cela est nécessaire aux exploitants de réseau ou aux fournisseurs de services à des fins opérationnelles.

7.5. Les données contenues dans un annuaire peuvent être utilisées par les exploitants de réseau ou les fournisseurs de services à des fins de gestion d'un service de renseignements portant sur des demandes ponctuelles. Tout renseignement devrait être limité à la communication des données figurant dans l'annuaire. Des mesures devraient être prises pour lutter contre les abus. Le service de renseignements ne devrait pas fournir d'informations relatives aux abonnés ne figurant pas dans l'annuaire sauf avec leur consentement écrit et éclairé.

7.6. L'utilisation des données figurant dans l'annuaire est au surplus régie par les principes pertinents de la Recommandation N° R (91) 10 sur la communication à des tierces personnes de données à caractère personnel détenues par des organismes publics.

b. Utilisation des données à des fins de marketing direct

7.7. Les principes de la Recommandation N° R (85) 20 sur la protection des données à caractère personnel utilisées à des fins de marketing direct s'appliquent à l'utilisation par des tiers des données d'abonnés à des fins de marketing direct.

7.8. Le droit interne devrait établir des garanties appropriées et déterminer les conditions selon lesquelles les données des abonnés peuvent être utilisées par les exploitants de réseau, les fournisseurs de services et par des tiers à des fins de marketing direct par téléphone ou par d'autres moyens de télécommunication.

7.9. L'élaboration de codes de conduite devrait être encouragée afin d'assurer que la pratique utilisée ne cause pas de gêne aux abonnés. En particulier, le droit interne ou les codes de conduite devraient porter sur les heures auxquelles le démarchage par téléphone peut être fait, la nature des messages et la manière dont ils sont transmis.

7.10. Le marketing direct par téléphone ou par d'autres moyens de télécommunication ne peut être pratiqué à l'égard d'un abonné qui a exprimé le souhait de ne pas recevoir de messages publicitaires. A cette fin, il conviendrait de développer des moyens appropriés pour identifier les abonnés qui ne souhaitent pas faire l'objet de messages publicitaires par téléphone.

7.11. Les automates d'appels visant à transmettre des messages pré-enregistrés de nature publicitaire ne peuvent être transmis qu'à des abonnés ayant donné leur consentement exprès et éclairé aux fournisseurs de ce service. L'abonné peut retirer son consentement à tout moment.

c. Facturation détaillée

7.12. Les exploitants de réseau et les fournisseurs de services ne devraient mettre des factures détaillant les numéros des abonnés appelés à la disposition d'un abonné qu'à sa demande. Il devrait être tenu compte de la vie privée des co-utilisateurs et des correspondants.

7.13. Les données nécessaires à la facturation ne devraient pas être conservées par les exploitants de réseau ou par les fournisseurs de services pendant une durée dépassant les délais strictement nécessaires au paiement, tout en gardant à l'esprit la nécessité éventuelle de conserver les données pendant une durée raisonnable en vue de réclamations liées à la facturation ou si des dispositions légales exigent la conservation de ces données plus longtemps.

d. Téléphonie interne

7.14. En principe, les individus devraient être informés, par des moyens appropriés, du fait que les données résultant de l'utilisation d'un téléphone sont collectées et traitées par le titulaire de la ligne. Les données devraient être effacées immédiatement après paiement de la facture.

7.15. Les principes énoncés dans la Recommandation N° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi s'appliquent à l'utilisation par les employeurs d'autocommutateurs téléphoniques sur les lieux de travail.

e. Identification de la ligne d'appel

7.16. L'introduction d'une caractéristique technique permettant de visualiser le numéro de téléphone d'un appel entrant sur le terminal de l'abonné appelé devrait être accompagnée d'informations destinées à tous les abonnés indiquant que cette caractéristique est disponible pour certains abonnés et que, de ce fait, il est possible que leur numéro de téléphone soit révélé à l'abonné appelé.

L'introduction de cette caractéristique devrait être accompagnée de la possibilité pour l'abonné appelant de supprimer par un moyen simple l'affichage de son numéro de téléphone sur le terminal de l'abonné appelé.

7.17. Le droit interne devrait déterminer les conditions et garanties selon lesquelles les exploitants du réseau sont autorisés ou obligés d'outrepasser la décision de l'appelant visant à supprimer l'affichage de son numéro sur l'écran du terminal de l'appelé.

f. Transfert d'appel

7.18. Il conviendrait d'étudier la possibilité de mécanismes permettant à un tiers abonné d'obtenir l'annulation d'un transfert d'appel en cas de désaccord.

7.19. Lorsque, en accord avec les dispositions du principe 2.4 relatif à l'interception des communications, la surveillance ou l'interception des appels entrants et sortants d'un abonné est autorisée, les mesures de surveillance ou d'interception ne devraient pas s'étendre à tous les appels entrants sur le terminal du tiers abonné mais uniquement à ceux qui font l'objet d'un transfert.

g. Téléphonie mobile

7.20. En ce qui concerne la fourniture et l'exploitation d'un service de téléphonie mobile, les exploitants de réseau et les fournisseurs de services devraient informer les abonnés des risques d'atteinte au secret de la correspondance qui peuvent accompagner l'utilisation des réseaux de téléphones mobiles, en particulier en l'absence de chiffrement des communications radio. Des moyens permettant aux abonnés aux réseaux de téléphones mobiles le chiffrement de leurs communications ou offrant des garanties équivalentes devraient être mis au point.

7.21. Il faudrait accorder de l'attention à la nécessité d'assurer que la facturation de l'utilisation d'un téléphone mobile n'exige pas l'enregistrement de données révélant la localisation trop précise de l'abonné ou de la partie appelée au moment de son utilisation.

Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données*

(Modèles de clauses pour inclusion dans un contrat type)

élaboré conjointement par

Le Conseil de l'Europe
La Commission des Communautés européennes
La Chambre de Commerce Internationale

Le concédant et le cessionnaire conviennent de procéder à une concession du droit d'usage de données à caractère personnel, contre paiement d'une somme de ...

Les conditions suivantes régissent l'accord entre les parties :

1. Obligation du concédant

Le concédant déclare et garantit au cessionnaire que les données sont transférées licitement au cessionnaire et que, conformément au droit interne, elles

a. ont été obtenues et traitées loyalement et licitement;

b. ont été enregistrées pour des finalités déterminées et légitimes et ne sont pas employées de manière incompatible avec ces finalités;

c. sont adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles seront concédées;

d. sont exactes et à jour;

e. bénéficient d'une autorisation de conservation pour une durée de ...

2. Obligations du cessionnaire

Le cessionnaire déclare et garantit pour sa part que l'usage qu'il fera des données respectera en tous points les principes énoncés dans les déclarations et garanties du concédant et qu'il s'interdira tout traitement ou usage des données qui serait contraire au contrat. A cet effet, et sans que cette énumération soit limitative, le cessionnaire s'engage en particulier à respecter les obligations suivantes :

a. le cessionnaire fera usage des données pour les finalités suivantes, à l'exclusion de toutes autres, à savoir : (*les énumérer*);

b. le cessionnaire s'interdit de traiter des données à caractère personnel révélant l'origine raciale, les origines politiques ou les convictions religieuses ou autres,

* Le commentaire explicatif relatif à ce contrat-type peut être obtenu en français et en anglais auprès du secrétariat du Préposé fédéral à la protection des données.

ainsi que toutes données à caractère personnel concernant la santé ou la vie sexuelle ou le casier judiciaire, à moins que ce traitement ne soit régi par les garanties qui auraient été appliquées en vertu du droit interne du concédant;

c. le cessionnaire exploitera les données exclusivement pour son usage personnel et ne communiquera les données gratuitement ou contre paiement, à aucune autre personne morale ou physique, sauf en cas d'obligation prévue par son droit interne et mentionnée expressément;

d. le cessionnaire rectifiera, effacera et mettra à jour immédiatement les données, dès qu'il aura reçu les instructions à cet effet du concédant. Le cessionnaire s'engage en particulier à rectifier, compléter ou effacer tout ou partie des données s'il s'avère que ces mesures sont requises par la loi de l'Etat du concédant ou sont fondées sur des circonstances nouvelles intervenues dans l'Etat du concédant, circonstances que le concédant notifiera et justifiera au cessionnaire dès qu'une annonce légale paraîtra dans l'Etat du concédant.

Le cessionnaire s'engage à garantir aux personnes concernées le droit d'accès à leurs données ainsi que le droit de rectification et d'effacement de celles-ci dans le mêmes conditions qu'en vertu du droit interne du concédant.

Au cas où le cessionnaire refuserait de permettre aux personnes concernées d'exercer le droit d'accès ou refuserait la rectification ou l'effacement demandé(e) par la personne concernée, le concédant :

- résiliera purement et simplement le contrat, dans les conditions et avec les conséquences en résultant selon ce que prévoit la clause 5, ou
- déclenchera la procédure de désignation d'un arbitre prévue par la clause 4.

3. Responsabilité et indemnisation

Le cessionnaire est responsable de l'usage qui est fait des données transmises par le concédant.

Le cessionnaire s'engage à indemniser le concédant pour tout manquement à ses obligations résultant du contrat ou pour toute faute ou toute négligence manifeste liée à l'exécution du contrat.

4. Règlement des conflits

extraits du rapport explicatif :

37. Les parties au contrat-type ou à un contrat incluant les modèles de clauses doivent prévoir un système approprié de règlement des conflits découlant de l'exécution du contrat-type ou des modèles de clause.

Elles peuvent soumettre leurs litiges à l'arbitrage ou à l'expertise.

38. Si les parties au contrat conviennent de recourir à l'arbitrage pour régler leurs différends, elles peuvent se référer aux règles d'arbitrage en vigueur de la CNUDCI ou de la CCI et appliquer les règles modèles de ces Organisations.

Clause arbitrale (CNUDCI) :
"Tout litige, controverse ou réclamation né du présent contrat ou se rapportant au présent contrat ou à une contravention au présent contrat, à sa résolution ou à sa nullité, sera tranché par voie d'arbitrage conformément au Règlement d'arbitrage de la CNUDCI actuellement en vigueur."

Clause arbitrale (CCI) :
"Tous différents découlant du présent contrat seront tranchés définitivement suivant le Règlement de conciliation et d'arbitrage de la Chambre de Commerce Internationale par un ou plusieurs arbitres nommés conformément à ce Règlement."

Il est recommandé d'ajouter certains éléments à ces clauses compromissoires modèles comme :

- *la langue utilisée lors de l'arbitrage*
- *le lieu de l'arbitrage*
- *le nombre d'arbitres.*

Cependant, si le contrat n'a pour unique objet que des flux transfrontières de données, les parties peuvent stipuler la procédure suivante de nomination des arbitres :

"Chaque partie nommera un arbitre, les arbitres ainsi nommés conviendront d'un troisième arbitre choisi sur une liste de personnes sélectionnées par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel[*] , qui sera le président du tribunal arbitral. Dans le cas où les arbitres nommés par les parties n'arrivent pas à se concerter sur la nomination d'un troisième arbitre dans les trente jours, la CCI (ou l'autorité de nomination choisie par les parties pour l'arbitrage) nommera le troisième arbitre conformément à ses règles d'arbitrage."

Le cas échéant, cette clause peut également être utilisée pour des contrats mixtes.

39. Si le contrat comporte des clauses sur les flux transfrontières de données, mais n'est pas limité à cet objet, les parties peuvent recourir à une expertise dans ce domaine pendant la procédure principale arbitrale.

Dans de telles circonstances, les parties pourraient prévoir que l'expert à nommer sera sélectionné sur une liste de personnes établie par le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel. Cet expert rendra un avis au tribunal arbitral.

[*] La liste des arbitres peut être obtenue auprès du Secrétariat du Conseil de l'Europe.

5. Résiliation du contrat

S'il s'avère que le cessionnaire fait preuve de mauvaise foi dans l'exécution du contrat ou refuse de respecter notamment la décision des arbitres, le concédant se réserve le droit de résilier le contrat par lettre recommandée avec avis de réception, ou par tout autre moyen équivalent, sans préjudice d'une éventuelle demande de dommages-intérêts.

Au moment de la résiliation du contrat, le cessionnaire doit détruire les données et en informer le concédant en conséquence.

En cas de manquement à la clause précédente, le cessionnaire s'engage à verser au concédant la somme de ...

Droit applicable (extrait du rapport explicatif)

25. Les parties sont libres de choisir le droit applicable au contrat entre le concédant et le cessionaire. Elles devraient toujours stipuler expressément le droit qu'elles ont choisi. Lorsque le droit interne applicable assure une meilleure protection des données à caractère personnel, il est recommandé au concédant de vérifier s'il doit compléter les clauses en conséquence.