Préposé fédéral à la protection des données

Rapport d'activités 1999/2000

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 1999 au 31 mars 2000.

TABLE DES MATIÈRES

* : Version originale en allemand

* : Version originale en allemand

* : Version originale en allemand

* : Version originale en allemand

AVANT PROPOS

Le 21ème siècle s'ouvrira sous le signe de la communication électronique au niveau planétaire. Pour la protection des données, cette évolution est déjà devenue réalité, en partie du moins.

Le nombre et le volume des données en circulation ne cessent de croître. Les problèmes que pose la protection de ces données se multiplient en conséquence. Or, étant donné les multiples possibilités technologiques existantes, il est difficile, pour un individu non averti, de mesurer les risques qui accompagnent la communication de données personnelles. En effet, l'utilisation des nouvelles technologies permet un traçage de données de plus en plus important. La personne qui fournit des renseignements la concernant doit donc être consciente qu'elle donne en même temps à des tiers la possibilité d'établir un profil complet de son comportement, de ses déplacements, de ses habitudes de consommation ou autres. Il peut en résulter une fausse image de sa personnalité. En outre, il existe d'ores et déjà des méthodes permettant d'établir des profils individuels à partir des informations encore inutilisées figurant dans les fichiers. Ces méthodes d'analyse sont un excellent outil de marketing. Elles ouvrent par ailleurs la voie à une société où tous les faits et gestes des particuliers sont répertoriés.

Le progrès en matière de communication électronique ne doit pas primer les droits de la personnalité. Nous devons donc intégrer la protection des données aux systèmes d'information dès leur conception afin de réduire les risques liés aux réseaux mondiaux de données. Il faut créer des systèmes qui, d'une part, nécessitent un minimum de données et, de l'autre, permettent aux personnes concernées de faire effectivement valoir leurs droits.

La protection des données doit aussi mettre l'accent sur les moyens techniques d'autoprotection (par exemple les méthodes de cryptage) contre l'utilisation illicite des données. Il s'agit de donner aux individus eux-mêmes la possibilité de gérer, du moins en partie, les risques inhérents aux nouvelles techniques de communication.

Par ailleurs, il conviendra à l'avenir d'intégrer davantage de règles de protection des données dans des modèles d'autorégulation (par exemple les codes de conduite des associations). De plus, et indépendamment des réglementations nationales, la communication de données à l'étranger nécessitera une meilleure protection de la sphère privée, surtout par le biais d'accords internationaux.

Pour être effective, la prévention des risques inhérents aux nouvelles techniques de communication doit s'accompagner de mesures assurant une meilleure protection de la sphère privée (par exemple la promotion active des procédés de

cryptage par les personnes privées et les entreprises, le développement de programmes de cryptage destinés à tous les utilisateurs ou la mise en œuvre de projets permettant l'anonymat sur Internet).

La garantie de la sphère privée aura un impact déterminant sur l'accueil qui sera réservé aux nouvelles techniques de communication. Très bientôt, les produits et services nécessitant peu de données personnelles disposeront d'un atout majeur par rapport à ceux permettant un important traçage des données.

O. Guntern

REPERTOIRE DES ABREVIATIONS

ADN	Acide désoxyribonucléique
ASA	Association suisse d'Assurances
CAMS	Concordat des assureurs-maladie suisses
CC	Centrale de compensation
CDB 98	Convention relative à l'obligation de diligence des banques
CEDH	Convention européenne des droits de l'homme
CIM	Classification Internationale des Maladies, traumatismes et causes de décès
CJPD	Groupe de projet sur la protection des données
CNA	Caisse nationale suisse d'assurance en cas d'accidents
CP	Code pénal suisse
DCG	Délégation des Commissions de gestion
DFAE	Département fédéral des affaires étrangères
DOSIS	Système de traitement des données en matière de lutte contre le crime organisé
EDNA	Identification signalétique au moyen de profils d'ADN
FAMP	Système de traitement des données en matière de lutte contre la fausse monnaie, la traite des êtres humains et la pornographie
GEWA	Système de traitement des données en matière de lutte contre le blanchiment d'argent
IPAS	Système informatisé de gestion et d'indexation des dossiers et des personnes
ISIS	Système de traitement des données relatives à la protection de l'Etat
ISOK	Système de traitement des données en matière de lutte contre le crime organisé
LAMal	Loi fédérale sur l'assurance-maladie
LBVM	Loi sur les bourses
LFLP	Loi sur le libre passage
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
MEDAS	Centre d'observation médicale
ODR	Office fédéral des réfugiés
OFAS	Office fédéral des assurances sociales
OFE	Office fédéral des étrangers
OFP	Office fédéral de la police
OTVA	Ordonnance régissant la taxe sur la valeur ajoutée
RAI	Règlement sur l'assurance-invalidité
RNIS	Réseau numérique à intégration de services
T-PD	Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel
TPIY	Tribunal Pénal International pour l'ex-Yougoslavie
ZIS	Système central d'information

I. THEMES CHOISIS

1. Affaires de police

1.1. Sûreté intérieure: raccordement des cantons au système ISIS

L'ordonnance sur le système de traitement des données relatives à la protection de l'Etat a fait l'objet d'une révision totale. Cette révision entre dans le cadre du renforcement de la coopération Confédération–cantons grâce au raccordement des cantons au système ISIS. Consultés sur ce projet, nous avons émis un certain nombre de propositions.

Les organes cantonaux chargés de la sécurité ont été raccordés au système de traitement des données relatives à la protection de l'Etat (ISIS) afin de renforcer la coopération entre la Confédération et les cantons dans le domaine du maintien de la sûreté intérieure. Ce raccordement trouve sa base légale formelle dans la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Dans le cadre de ce raccordement des cantons, la police fédérale a procédé à la révision totale de l'ordonnance ISIS qui règle l'exploitation, la saisie des données ainsi que l'utilisation du système ISIS.

La nouvelle ordonnance défini notamment quelles données du système ISIS peuvent être consultées par les organes cantonaux de sûreté. Par contre, comme par le passé, seule la police fédérale reste habilitée à introduire des données dans le système ISIS. Un service de contrôle interne vérifie toutes les données saisie, en particulier l'indication des sources, l'appréciation de l'information et la durée de conservation.

Consultés par la police fédérale sur ce projet de révision, nous avons émis un certain nombre de propositions qui ont été acceptées et reprises dans le projet final. Il s'agissait notamment d'aspects touchant à certaines définitions, à la communication des données, au raccordement des cantons, aux durées de conservation des données ou encore au droit d'accès des personnes concernées. Cette nouvelle ordonnance ISIS est entrée en vigueur le 1er janvier 2000.

1.2. Exercice du droit d'accès « indirect » par les personnes concernées

En vertu de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, toute personne peut nous demander de vérifier si des données la concernant sont traitées conformément au droit par la police fédérale dans le système de traitement des données relatives à la protection de l'Etat (ISIS). Deux ans après l'entrée en vigueur de

cette nouvelle réglementation, une analyse de la mise en application de ce droit d'accès « indirect » peut être tirée en parallèle avec la procédure, en grande partie similaire, du droit d'accès « indirect » prévu dans la loi fédérale sur les Offices centraux de police criminelle de la Confédération (accès aux systèmes DOSIS, ISOK, FAMP et GEWA).

Un premier bilan avait été établi après neuf mois d'application de ce droit d'accès « indirect » (voir 6ème Rapport d'activités 1998/99 p. 225 ss). Une année après, un nouveau bilan peut être tiré sur les expériences faites non seulement dans le cadre de l'application de la réglementation sur le droit d'accès « indirect » conformément à la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), mais également sur celles faites par rapport à la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC).

A la trentaine de demandes d'accès déposées en application de la LMSI (accès au système ISIS de la police fédérale) viennent s'ajouter une dizaine d'autres demandes d'accès fondées cette fois sur la LOC (accès aux systèmes DOSIS, ISOK, FAMP et GEWA des services centraux). Cette loi prévoit un mécanisme d'accès « indirect » similaire à la LMSI, avec une approche encore plus restrictive puisque seul un libellé toujours identique peut être remis à la personne concernée.

La décision du Conseil fédéral de transférer en septembre 1999 la police fédérale du Ministère public de la Confédération à l'Office fédéral de la police (OFP) nous a amené à rechercher une procédure standard d'exercice de ce droit d'accès « indirect », que ces demandes visent les traitements de données de la police fédérale ou des services centraux. Nous avons donc élaborés, en collaboration étroite avec chacune de ces unités de l'OFP, une procédure claire et uniforme quant au déroulement de l'exercice de ces droits d'accès « indirects », en tenant compte des spécificités des deux lois à appliquer.

Les expériences faites dans le cadre de l'application de la LMSI et de la LOC ont été mises en commun et ont permis de finaliser tant les règles de procédure assurant une application adéquate de ce droit d'accès « indirect » que le mode de consultation des systèmes informatiques et des documents de dossiers existants éventuellement sur une personne demanderesse.

De l'analyse des expériences faites dans le cadre de l'application de ces réglementations sur le droit d'accès « indirect » peut être tiré le bilan suivant résumé en quatre points:

Premièrement le mécanisme mis en place ne correspond pas à un véritable droit d'accès indirect dans le sens où la personne concernée ayant déposée une

demande d'accès ne recevra en principe de notre part pour toute réponse à sa demande qu'un libellé toujours identique qui ne lui permettra pas de savoir si elle est enregistrée ou non. Deuxièmement, ce mécanisme nous permet en contrepartie d'exercer indirectement un contrôle plus régulier sur les traitements de données effectués par la police fédérale et les services centraux de l'OFP. Troisièmement, il convient de relever que cette tâche implique un important investissement de nos ressources pour pouvoir traiter chaque demande conformément aux exigences légales. Enfin, bien que de nombreuses règles ont pu être mises en place avec l'OFP pour appliquer ces dispositions, nous allons, parallèlement au traitement des demandes d'accès qui nous sont adressées, poursuivre la recherche de solutions aux problèmes juridiques et procéduraux encore pendants en collaboration avec l'OFP.

1.3. Projet « Nouveau passeport suisse »

Le nombre de falsifications du passeport suisse, modèle 1985, augmente. Contrairement aux passeports de la majorité des pays européens limitrophes, ce passeport ne peut pas être lu de manière automatisée. C'est pourquoi le chef du Département fédéral de justice et police a mandaté à fin novembre 1998 une commission avec la mission de concevoir un nouveau passeport suisse et d'élaborer une loi fédérale sur les documents d'identité.

Le Préposé fédéral à la protection des données fut représenté aussi bien dans la commission que dans le groupe de travail « Droit ». La plupart du temps, le travail fut entre autres guidé par le désir de régler de manière transparente et claire les aspects importants liés au traitements nécessaires de données personnelles. En prévision d'une future banque centrale qui devait être créée au niveau fédéral, on s'inspira au début des objectifs, des contenus et des conditions de la banque de données IDK (carte d'identité) gérée à l'Office fédéral de la police. Etant donné que cette dernière avait été conçue uniquement comme base de données administrative, on présuma longtemps que la banque de données devant être créée aurait également la fonction d'une simple base de données administrative. Ce but n'avait pas été déclaré de manière explicite dans le projet de loi, mais il fut reflété dans les accès initialement prévus. Contrairement à notre objection relevant que la base de données administrative deviendrait une banque de données utilisée pour les recherches policières, on a choisi d'octroyer des accès aussi bien aux corps des gardes-frontière qu'aux polices des frontières. Bien que nous ayons défendu notre position jusqu'à la fin, la commission a maintenu les accès étendus aux corps des gardes-frontière et aux polices des frontières. Par la suite, nous devions apprendre que le Département fédéral de justice et police a écarté la décision de la commission et a encore une fois étendu les accès pour inclure également les organes fédéraux de police (Police

fédérale et Offices centraux de police criminelle). D'autre part, la demande d'ouverture de la procédure de consultation a été soumise de manière incomplète au Conseil fédéral puisque on y a mentionné uniquement notre position défavorable concernant les accès octroyés aux corps des gardes-frontière et aux polices des frontières. Notre intervention écrite concernant la procédure ainsi que l'extension des accès à la Police fédérale et aux Offices centraux de police criminelle n'a été aucunement mentionnée. Nous nous sommes donc vu contraints d'attirer l'attention sur ce fait dans la procédure de corapport au Conseil fédéral.

1.4. Le projet « Casino 2000 »

« Casino 2000 » est le nom du projet qui traite de l'élaboration des dispositions d'exécution relatives à la loi fédérale sur les jeux de hasard et les maisons de jeu. L'ordonnance sur les jeux de hasard et les maisons de jeu (ordonnance sur les maisons de jeu) a été soumise à la consultation des offices à fin 1999.

Notre objectif lors de notre participation à l'élaboration de l'ordonnance sur les maisons de jeu était que des dispositions:
- fixent de manière suffisante quelles sont les données personnelles devant être traitées par les maisons de jeu ainsi que par la commission des maisons de jeu,
- décrivent la nature et la manière de ces traitements de données ainsi que les circonstances dans lesquelles ils sont effectués et
- règlent les délais de conservation.

Dans ce contexte, il s'est une nouvelle fois avéré qu'il est indispensable que des analyses des tâches et de l'organisation soient effectuées avant d'entamer l'élaboration de bases légales. Le but et le sens de telles analyses est d'établir et de définir qui doit remplir quelles tâches, quelles sont les données absolument nécessaires à l'accomplissement de ces tâches et qui doit traiter quelles données dans le cadre de l'accomplissement de sa tâche. Il y a lieu également d'examiner quels flux de données sont nécessaires au sein d'une unité ou même vers des tiers, comment les traitements de données doivent être effectués du point de vue de l'opportunité et de la proportionnalité et combien de temps les données doivent être conservées.
Si ces réflexions ne sont pas faites avant l'élaboration d'une base légale, ceci a pour conséquence – comme c'est le cas pour la loi sur les maisons de jeu – qu'il n'existe du point de vue de la protection des données pas de base légale suffisante pour le traitement de données personnelles sensibles par les maisons de jeu. Le fait qu'aucune analyse des tâches et de l'organisation n'ait été faite avant d'élaborer la base légale mène à une situation où l'on dépense beaucoup

de temps et d'énergie pour élaborer des projets qui s'avèrent incomplets et qui doivent ensuite laborieusement être remaniés.
Finalement, l'ordonnance sur les maisons de jeu a été standardisée de manière plus ou moins satisfaisante, surtout si l'on prend en considération qu'il s'agit en partie d'approches toutes nouvelles. Ainsi, on y a défini quelles sont les données que la commission des maisons de jeu traitent, quelles sont les informations que les maisons de jeu sont autorisées à traiter dans le cadre du concept social, du concept de sécurité ainsi que lorsqu'un client pénètre dans une maison de jeu. A notre avis, il serait souhaitable après un certain temps de procéder à un nouvel examen de la possibilité d'apporter des précisions à cette ordonnance.
Nous maintenons d'autre part notre exigence que lors d'une prochaine révision de la loi soit créée une base légale suffisante pour le traitement de données personnelles sensibles par les maisons de jeu en rapport avec le concept social.

1.5. Ordonnance sur le casier judiciaire automatisé

En même temps que la révision du Code pénal suisse, l'ordonnance sur le casier judiciaire informatisé est entrée en vigueur le 1er janvier 2000.

Le paquet de lois de l'Office fédéral de la police qui réglait la période transitoire prévue par la loi sur la protection des données pour l'élaboration des bases légales pour le traitement de données personnelles sensibles (voir notre 5ème Rapport d'activités 1997/98, page 148) prévoyait la révision des dispositions du Code pénal suisse relatives au casier judiciaire. Ces dispositions sont entrées en vigueur le 1er janvier 2000. En même temps, l'ordonnance sur le casier judiciaire informatisé est entrée en vigueur.
Nous avons eu très tôt la possibilité de défendre les intérêts de la protection des données. Lors de l'appréciation du projet, nous devions cependant prendre en compte le fait que la nouvelle ordonnance devait aller dans la direction des dispositions légales nouvellement créées du Code pénal suisse, dispositions entrées en vigueur le 1er janvier 2000. L'objectif de ces dernières n'était pas de revoir le droit matériel relatif au casier judiciaire. Il s'agissait plutôt de prendre en compte les exigences de la loi sur la protection des données et de créer une base légale suffisante pour le droit relatif au casier judiciaire existant. La conséquence fut que des intérêts majeurs de la protection des données telles que les exceptions au droit d'accès pour la protection de la personne concernée ont pu être prises en compte dans l'ordonnance, étant donné qu'elles avaient déjà été considérées lors de la révision du Code pénal. D'autres demandes de la protection des données n'ont cependant pas pu être prises en compte dans l'ordonnance. C'est le cas de la suppression au lieu de la radiation simple des enregistrements concernant des actes qui étaient punissables au moment où ils

ont été commis, mais qui suite à une évolution des valeurs morales de notre société ne font plus aujourd'hui l'objet de sanctions pénales. A cet égard, nos espoirs se portent sur les travaux de révision encore en cours de la partie générale du CP.

2. Droit des étrangers et droit d'asile

2.1. Traitement des données par la section nationalité

Dans le cadre de la réforme du gouvernement et de l'administration, la section nationalité de l'Office fédéral de la police a été transférée à l'Office fédéral des étrangers. La nouvelle réglementation relative au traitement des données dans le système informatisé de gestion et d'indexation des dossiers et des personnes de l'Office fédéral de la police ne pouvant, contrairement à ce qui avait été prévu, s'appliquer à la section nationalité, nous avons été consultés sur la solution juridique à adopter. Notre proposition d'élaborer des dispositions de protection des données dans la loi fédérale sur la nationalité et d'introduire ce projet de révision dans le message concernant la création et l'adaptation des bases légales nécessaires au traitement de données personnelles a permis de régler de manière adéquate ce problème.

Le Parlement a adopté en juin 1999 le cadre légal formel nécessaire au traitement des données dans le système informatisé de gestion et d'indexation des dossiers et des personnes (IPAS) de l'Office fédéral de la police (OFP) en créant une nouvelle disposition dans le code pénal. Au cours de cette même année, suite aux travaux liés à la réforme du gouvernement et de l'administration, la section nationalité, jusqu'alors unité de l'OFP, a été transférée à l'Office fédéral des étrangers (OFE). Ce transfert a notamment eu pour conséquence que les nouvelles dispositions légales du code pénal pour le traitement des données de l'OFP ne pouvaient plus, contrairement à ce qui avait été prévu à l'origine dans le message du Conseil fédéral, s'appliquer à la section nationalité de l'OFE.

Consultés par le Secrétariat général du Département fédéral de justice et police sur la recherche de solution juridique, nous avons relevé que durant les débats parlementaires, la disposition relative au traitement des données en matière de nationalité avait de toute façon déjà été biffée de la base légale du système IPAS.

Dans l'optique de trouver une solution juridiquement irréprochable et réalisable dans les meilleurs délais et qui autorise également le traitement de données sensibles, nous avons proposé qu'un chapitre spécifique au traitement des données personnelles soit introduit dans la loi fédérale sur la nationalité. Des dispositions ont alors été élaborées portant sur le traitement des données personnelles, l'exploitation d'une banque de données informatisée, la communication des données ainsi que les accès par procédure d'appel. Afin de permettre une adoption rapide de ce projet, nous avons proposé de saisir l'opportunité d'intégrer cette révision de la loi sur la nationalité dans le message concernant la création et l'adaptation des bases légales nécessaires au traitement de données personnelles qui était en cours d'élaboration.

Tant le Département fédéral de justice et police que l'OFE et l'Office fédéral des réfugiés ont approuvé nos propositions.

3. Télécommunications et poste

Télécommunications

3.1. Le droit à la protection des données dans le domaine des télécommunications

« Un coup de fil, c'est si facile ». Ce spot publicitaire bien connu exprime à souhait le fait que la télécommunication est, malgré sa complexité, devenue un acte banal de notre société. Acte banal, mais pas anodin. Lors de l'utilisation d'un téléphone, d'un fax ou d'un courrier électronique, nous laissons des traces qui augmentent le risque de traitement abusif et favorisent la constitution de vastes profils de la personnalité. Les télécommunications sont ainsi susceptibles de mettre en jeu la vie privée des usagers et la confidentialité de leurs relations. Chaque usager doit être conscient qu'il a des droits et des moyens de se protéger. Il peut s'immiscer dans le processus de traitement de ses données et ainsi déterminer si des données personnelles à son sujet peuvent être collectées et traitées, par qui, dans quelle ampleur, pour quelles finalités, pour quelle durée et à qui elles peuvent être communiquées.

Face à la globalisation des échanges d'information et aux facilités offertes par les technologies actuelles de télécommunication, l'individu doit demeurer un partenaire actif dans la définition des traitements de données qui le concernent. Il doit pouvoir attribuer ou déterminer la valeur qu'il attache à ses propres

données et l'utilisation qu'il tolère d'autres personnes. Il assume ainsi également une responsabilité dans la définition de la protection qu'il entend exiger pour lui-même et dans l'exercice des droits que lui confère la loi. Outre les différents droits qui découlent de la LPD et notamment le droit à l'information sur les traitements, le droit de s'opposer au traitement, le droit d'accès aux données le concernant, le droit de rectification et le droit d'ester en justice, l'individu peut faire valoir différents droits qui découlent notamment du droit des télécommunications. Des restrictions de ces droits sont néanmoins possibles notamment en cas d'abus ou d'actes illicites.

Secret des télécommunications

Toute personne a droit au secret de ses télécommunications personnelles. Les fournisseurs de services sont tenus de prendre les mesures nécessaires propres à garantir le respect de la confidentialité des communications. Ils doivent également informer les usagers sur les risques et les moyens de se protéger. L'obligation de secret couvre toutes les données personnelles liées à l'utilisation d'un service de télécommunication ou qui transitent par un tel service. Il s'agit en particulier des données de contenu et des données de trafic (données accessoires). Les données enregistrées dans le fichier client du fournisseur de services de télécommunication ne sont pas couvertes par le secret des télécommunications, dans la mesure où elles ne sont pas couplées avec les données de contenu ou de trafic.

Droit à l'anonymat

La meilleure garantie du respect du droit à la protection des données peut être donnée en évitant de collecter et de traiter des données personnelles. La personne concernée peut ainsi se protéger en évitant de divulguer des informations à son sujet. Conformément aux principes de proportionnalité et de finalité, seules les données absolument nécessaires doivent être traitées. Ainsi, toute personne devrait pouvoir être en mesure d'exiger des fournisseurs de services que les systèmes soient conçus de façon à permettre une utilisation des installations de télécommunication qui limitent au strict nécessaire le recours à des données personnelles. Cet objectif peut être atteint par l'utilisation de pseudonymes ou par la mise à disposition de dispositifs anonymes d'accès au réseau et aux services de télécommunication. Cela implique en particulier le maintien de cabines téléphoniques avec des cartes à prépaiement, l'introduction d'installations téléphoniques fixes et la possibilité d'utiliser des téléphones mobiles avec de telles cartes (voir 5e Rapport d'activités 1997/98, p. 168), la possibilité de ne pas faire afficher le numéro appelé ou appelant, le droit de ne pas figurer dans les annuaires téléphoniques et la possibilité d'exiger des factures détaillées sans pouvoir identifier les numéros appelés ou appelants. A

l'instar de la législation allemande, il serait souhaitable d'introduire dans le droit positif suisse une disposition garantissant le droit à l'anonymat.

Annuaire téléphonique

Seules les données nécessaires à identifier raisonnablement celui qui souhaite figurer dans un annuaire téléphonique et à empêcher la confusion avec d'autres personnes devraient y être enregistrées. D'autres données ne devraient y être introduites qu'à la demande expresse de la personne concernée. Le choix de l'usager ne doit pas se limiter à la possibilité de figurer ou de ne pas figurer dans un annuaire et de déterminer quelles données il veut y voir publiées. Il doit également pouvoir choisir en fonction du type d'annuaire proposé par les fournisseurs de services de télécommunication. En effet aujourd'hui, l'annuaire n'est plus uniquement publié sous forme papier. Il est disponible sur des supports informatiques (CD-Rom, disquettes), voire accessible par procédure d'appel, notamment sur Internet. Les technologies permettent également de procéder à des recherches selon différents critères ou même à des recherches inversées (recherche par le numéro d'appel), de coupler les annuaires à d'autres fichiers (par exemple à un système d'information géographique) ou d'établir des listes. Actuellement le choix offert à l'abonné est insuffisant. Il ne peut, par exemple, pas figurer uniquement sur un annuaire papier et refuser de figurer sur un annuaire électronique. A moins qu'il ne soit enregistré dans aucun annuaire, il ne peut empêcher la recherche inversée ou par l'adresse. Il ne peut également pas s'opposer à ce qu'un annuaire soit télédéchargé pour être publié sur Internet. Ainsi, à l'instar de l'astérisque (*) pour l'interdiction de la prospection commerciale, il conviendrait de marquer les abonnés qui ont refusé la publication sur Internet ou sur un support électronique, tel qu'un CD-Rom ou encore qui se sont opposés au traitement de leurs données par un service de recherche inversé.

Prospection commerciale

Face à la prospection commerciale par téléphone ou l'envoi de messages SMS, l'indication dans l'annuaire à l'aide de l'* est insuffisant, car certaines firmes procèdent à des appels aléatoires et recourent à des systèmes automatisés d'appels sans intervention humaine. En l'absence de mesures techniques permettant de refuser de tels appels ou les rendant impossibles, il conviendrait de requérir le consentement préalable des personnes concernées. à l'instar de la directive 97/66/CE du Parlement européen et du Conseil, du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

Facturation détaillée

L'abonné a le droit de recevoir des factures détaillées ou non. La facturation détaillée ne doit être établie que si l'abonné le demande. En pratique, certains fournisseurs de services de télécommunication établissent systématiquement des factures détaillées, sans que l'abonné l'ait demandé. Une facturation détaillée ne pose pas, en principe, de problèmes du point de vue de la protection des données, lorsque l'abonné qui la réclame, est le seul à utiliser le raccordement pour lequel la facture est établie et par conséquent connaît les numéros avec lesquels ils communiquent. Par contre, lorsque le raccordement est utilisé par plusieurs personnes, cela peut entraîner une atteinte à la vie privée des personnes appelées et des autres utilisateurs. De même si la facturation détaillée concerne un téléphone mobile, elle révèle non seulement les numéros appelés, mais également les numéros appelants, du moins lorsque l'abonné paye une partie de la communication. L'abonné qui reçoit une facturation détaillée est lui-même tenu de respecter la vie privée des co-utilisateurs de son raccordement et des personnes appelées ou appelantes. En particulier, il ne devrait pas utiliser les informations figurant sur sa facture à d'autres fins que la maîtrise de sa consommation téléphonique, de répartition des coûts ou de vérification de l'exactitude de la facture. Ainsi, il serait souhaitable de réintroduire la facturation détaillée sans le numéro d'appelé complet ou du moins de permettre aux usagers d'exiger que leur numéro ne figure pas sur une telle facture. Le numéro complet ne devrait être fourni qu'en cas de contestation, à des fins de preuve.

Affichage du numéro

Les fournisseurs de services téléphoniques et d'équipements téléphoniques offrent depuis quelques années des appareils permettant d'utiliser le réseau numérique à intégration de services (RNIS). Ces appareils offrent différentes possibilités et notamment permettent d'afficher le numéro appelé ou le numéro appelant (voir 1er Rapport d'activités 1993/94, p. 110; 2ème Rapport d'activités 1994/95, p. 144ss.; 4e Rapport d'activités 1996/97, p. 161ss.). Le numéro de téléphone est une donnée personnelle qui permet d'identifier la personne concernée. L'affichage du numéro apporte certes de nombreux avantages. Il peut néanmoins entraîner, dans certains cas, une atteinte à la personnalité. L'appelé est en mesure d'enregistrer les numéros et de les dépouiller par exemple à des fins commerciales. Il peut arriver que le numéro affiché sur l'appareil soit vu par des tierces personnes se trouvant dans l'entourage de l'appelé sans que celui-ci le veuille. Il est également possible de localiser géographiquement l'appel. La personne concernée doit ainsi pouvoir se protéger et déterminer si elle souhaite que son numéro et éventuellement d'autres données la concernant puissent être affichés, voire enregistrés lorsqu'elle téléphone ou lorsqu'elle est appelée. Elle doit pouvoir exercer ce droit de non affichage gratuitement, de manière permanente ou de cas en cas. De même l'appelé doit

avoir le droit de refuser de recevoir des appels non identifiés. Les entreprises de télécommunication doivent offrir à leurs abonnés la possibilité de supprimer l'affichage appel par appel ou de manière permanente. Elles doivent également leur offrir la possibilité de refuser les appels entrants non identifiés. Elles doivent les informer clairement de la manière d'exécuter ces opérations**.** Aujourd'hui le marché des télécoms offre déjà de nombreux appareils équipés de ces fonctionnalités. L'identification doit être maintenue pour les appels d'urgence. L'usager doit également respecter la vie privée des autres usagers. Il ne devrait en particulier pas conserver les numéros des personnes qui l'ont appelé et notamment les utiliser à d'autres fins que la communication avec ces personnes.

Déviation automatique des appels

Il est aujourd'hui possible de dévier son téléphone sur l'installation d'un tiers. Pour l'abonné qui procède à cette déviation, celle-ci n'est pas problématique pour autant que ce tiers en soit informé et soit disposé à prendre les appels. Si le tiers n'est pas averti, il doit être en mesure de mettre fin à la déviation, dans la mesure où cela est techniquement réalisable. Pour les personnes qui appellent, la déviation peut être problématique si elles ne s'attendent pas à communiquer avec une personne autre que l'abonné appelé. Il serait ainsi souhaitable qu'un signal acoustique ou visuel les prévienne de la déviation pour leur permettre le cas échéant de renoncer à la communication.

3.2. Révision de l'ordonnance sur les services de télécommunication

Dans le cadre de la révision de l'ordonnance sur les services de télécommunications, plusieurs dispositions ont été adaptées afin de mieux tenir compte des exigences de la protection des données. Il s'agit de la publication des numéros d'urgence pour lesquels la localisation est garantie dans tous les cas, de l'indication non détaillée dans certains cas des appels entrants et de la suppression gratuite de l'identification de la ligne appelante.

Nous avons été consultés par l'Office fédéral de la communication (OFCOM) dans le cadre de la procédure de révision de l'ordonnance sur les services de télécommunication (OST). Il s'est notamment exprimé sur les mesures de protection des raccordements installés à l'intérieur ou à l'extérieur des bâtiments, sur la nouvelle réglementation en matière d'appels d'urgence, sur les annuaires téléphoniques, sur les ressources d'adressage des appels entrants qui figurent sur les factures détaillées, sur la suppression de l'identification de la ligne appelante et enfin sur la statistique officielle en matière de télécommuni-

cations (voir également p. 144 Le droit à la protection des données dans le domaine des télécommunication). En ce qui concerne les questions touchant directement les utilisateurs des services de télécommunication, nous avons défendu les positions suivantes:

Appels d'urgence

L'accès aux services d'appels d'urgence (numéros 112, 117, 118, 143, 144 et 147) doit être possible à partir de n'importe quel raccordement. Dans le domaine de la téléphonie mobile, seul l'accès au service d'appel d'urgence 112 doit être assuré. La localisation d'un appel doit être garantie en ligne pour les numéros d'urgence 112, 117, 118 et 144 dans tous les cas (même si la personne a choisi de ne pas s'inscrire dans l'annuaire ou si elle a supprimé l'identification de la ligne appelante). L'OFCOM peut, sur demande, désigner d'autres numéros servant exclusivement à des services d'urgence (police, pompiers, services sanitaire et de sauvetage) pour lesquels la localisation des appels doit être garantie. Nous avons soutenu cette proposition en demandant que ces numéros soient alors rendus publics. Avant le 1er mai 2000, la réglementation était lacunaire et seuls la police et les pompiers pouvaient eux-mêmes désigner d'autres numéros d'urgences.

Annuaires téléphoniques

Le choix de l'abonné ne doit pas se limiter à la possibilité de figurer ou non dans un annuaire téléphonique et de déterminer, avec certaines restrictions, quelles données il veut y voir introduites. A l'heure actuelle, l'annuaire n'est plus uniquement disponible sous forme papier, on le trouve sur des supports électroniques comme les CD-ROM ou sur le réseau Internet. Il est possible de procéder à des recherches selon différents critères (canton, lieu, rue, partie du nom ou du prénom etc.) ou de manière inversée (obtenir un nom et une adresse au moyen de n'importe quel numéro de téléphone même tronqué). Il est également possible de coupler les annuaires à d'autres fichiers tels les fichiers de marketing ou de renseignements économiques. A l'instar des législations française et allemande, nous avons proposé d'introduire dans l'OST les droits pour l'abonné de ne pas figurer dans un annuaire distribué sur support électronique, de ne pas figurer dans un annuaire en ligne et de ne pas figurer dans un annuaire inversé. Le Conseil fédéral n'a pas retenu notre proposition.

Facture détaillée et données relatives aux appels entrants

Les abonnés sont de plus en plus appelés à régler des factures pour des appels entrants. C'est le cas du titulaire d'un numéro gratuit 0800 ou encore celui d'un abonné mobile recevant des appels à l'étranger. Afin de garantir la transparence de la facture, le projet de révision prévoyait que l'abonné puisse exiger de son

fournisseur la communication des ressources d'adressage des raccordements appelants y compris celles des personnes ne figurant pas dans l'annuaire ou ayant demandé la suppression de l'identification de la ligne. Une telle pratique viole le droit à la liberté personnelle et le droit à l'autodétermination individuelle. Elle va également à l'encontre du droit européen et des recommandations du Conseil de l'Europe qui exigent que la vie privée des co-utilisateurs et des correspondants soient prise en compte lors de l'élaboration de facture détaillée. L'intérêt de l'abonné à connaître les données nécessaires au paiement de la facture se heurte au droit légitime du correspondant à la protection de sa vie privée. L'OFCOM a jugé cependant l'intérêt de l'abonné supérieur à celui du correspondant. Pour cette raison l'OFCOM a défendu l'indication des numéros de téléphone sans restriction des appels entrants. Nous avons proposé l'indication non détaillée (indication du type de raccordement et du numéro amputé au moins des quatre derniers chiffres) pour les personnes ne figurant pas dans l'annuaire, celles ayant supprimés l'identification de la ligne et celles s'étant formellement opposés à la communication des ressources d'adressage. Cette solution tient compte de l'intérêt de l'abonné (il peut constater qu'il a reçu un appel pour lequel il doit payer tout ou partie du coût) sans pour autant heurter l'intérêt du correspondant. Le Conseil fédéral a suivi la proposition du PFPD. Dès le 1er mai 2000, sur demande de l'abonné, les ressources d'adressages des raccordements appelants figurent sur les factures de manière non détaillée.

Suppression de l'identification de la ligne appelante (service CLIR)

Depuis le 1er mai 2000, les fournisseurs de services de télécommunication doivent offrir à leurs abonnés, par un moyen simple et gratuit, la possibilité de supprimer, appel par appel, ou en permanence, l'affichage de l'identification de leur ligne sur l'installation de l'abonné appelé. Cela fait de nombreuses années que nous demandions la gratuité du service CLIR. Cette disposition de l'OST est enfin conforme aux dispositions de protection de la personnalité et des données ainsi qu'au droit européen (voir également p. 151).

3.3. Confusion entre deux clients lors de l'envoi de la facture détaillée

Les données accessoires de télécommunication figurant sur les factures détaillées sont soumises à l'obligation d'observer le secret. L'envoi à un tiers de telles données viole non seulement les dispositions de protection des données mais également le secret des télécommunications.

Plusieurs personnes se sont adressées à notre secrétariat pour nous signaler que leur fournisseur de services de télécommunication leur avait adressé des factures détaillées concernant des tiers parfois homonymes.
Nous avons informé les fournisseurs en question que les données figurant dans les factures détaillées (numéros appelés, début et durée de la conversation, montant etc.) sont des données accessoires de télécommunication soumis à l'obligation d'observer le secret (secret des télécommunications). Il est ainsi interdit à un fournisseur de services de télécommunication de donner à des tiers des renseignements sur les communications d'un de ses clients; de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers. En matière de protection des données, le maître de fichiers doit prendre toutes les mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre tout traitement non autorisé (communication à des tiers non autorisés de données personnelles). Une erreur, toujours possible, est en principe excusable. Dans les cas en question, les fournisseurs ont continué d'envoyer les factures détaillées aux fausses personnes malgré plusieurs interventions des clients concernés. Nous avons rendu attentifs ces fournisseurs qu'ils violaient d'une part les principes généraux de la protection des données et d'autre part qu'ils s'exposaient aux sanctions pénales prévues en matière de violation du secret des postes et des télécommunications.

3.4. Jugement de la Commission fédérale de la protection des données concernant la perception d'une taxe pour la suppression de l'identification de la ligne appelante

La controverse qui règne au sujet de la perception d'une taxe pour la suppression de l'identification de la ligne appelante est enfin réglée. Dans son jugement du 12 mars 1999, la Commission fédérale de la protection des données a constaté que c'est en violation du droit en vigueur jusqu'au 31 décembre 1997 que le Département fédéral des Transports, des Communications et de l'Energie (actuellement Département fédéral de l'Environnement, des Transports, de l'Energie et de la Communication) et Télécom PTT (actuellement Swisscom SA) ont décidé de percevoir une taxe pour l'installation du service de suppression de l'identification de la ligne appelante. Depuis le 1er mai 2000, ce service est gratuit.

Le thème de l'affichage (service CLIP) et surtout de la suppression de l'affichage du numéro de l'appelant (service CLIR) nous occupe depuis plusieurs années. Il aura fallu attendre l'an 2000 pour enfin parvenir au but poursuivi par le Préposé fédéral: donner aux abonnés, par un moyen simple et

gratuit, la possibilité de supprimer, appel par appel ou en permanence, l'affichage de l'identification de la ligne appelante.
Dans son jugement du 12 mars 1999, la Commission fédérale de la protection des données (CFPD) rappelle que le Conseil fédéral a admis la prise en considération des droits étrangers et européens s'agissant de la protection de la personnalité. Dans le domaine des télécommunications, la législation européenne et la législation allemande par exemple prévoient la gratuité du service CLIR. La CFPD note que le droit à la suppression de l'identification de la ligne appelante est un droit protecteur de la personnalité dans le domaine du traitement des données et que son exercice peut être empêché par la perception d'un émolument. La CFPD souligne que les droits reconnus par les dispositions de la LPD (droit d'opposition et opposition à la communication de données personnelles traitées par des organes fédéraux) ne sont pas subordonnés au paiement d'un émolument. La CFPD constate qu'avant l'entrée en vigueur du nouveau droit des télécommunications il n'existait pas de base légale autorisant la perception de la taxe et que les personnes désireuses de garder la maîtrise de leurs données étaient obligées de payer dès lors que le service CLIP était automatiquement mis en place. La CFPD a renoncé à examiner la constitutionnalité et la légalité de la disposition de l'ordonnance sur les services de télécommunication prévoyant la perception d'une taxe pour le service CLIR. Cette disposition a été révisée et, depuis le 1er mai 2000, le service CLIR est gratuit. Du point de vue du droit de la personnalité et des droits fondamentaux, il est réjouissant de constater que la personne appelée et la personne appelante ont la même possibilité d'utilisation des services CLIP et CLIR.

Poste

3.5. La mise à jour d'adresses postales avec Mat[CH]move

Quiconque déménage, aimerait continuer à recevoir à son nouveau domicile les lettres et paquets qui lui sont adressés, rapidement et sans problèmes. Avec la demande de réexpédition, la Poste Suisse offre la possibilité à ses clients de se faire retransmettre le courrier qui est encore adressé à l'ancienne adresse. Les traitements de données relatifs à cette retransmission n'étaient pas conformes en plusieurs points aux exigences de la législation sur la protection des données et ont provoqué une certaine irritation auprès des clients.

Se faire réexpédier le courrier postal par l'intermédiaire de l'ancienne adresse pendant une durée prolongée est un procédé inefficace et coûteux. Il y a donc lieu de communiquer aussi rapidement que possible la nouvelle adresse aux

expéditeurs. Ceci peut être fait par le client lui-même, sinon les expéditeurs demandent la nouvelle adresse auprès de la Poste. C'est dans ce but que la Poste offre – en collaboration avec sa filiale Data Center Luzern AG (DCL) – le service Mat[CH]move, qui permet aux entreprises de mettre à jour périodiquement leurs fichiers d'adresses.

Même si la mise à jour d'adresses peut ne pas être considérée comme une communication de données à des tiers, elle représente sans aucun doute un traitement de données personnelles que la personne concernée est en droit d'interdire à tout moment. Depuis le début de 1998, la Poste est soumises aux dispositions de la loi sur la protection des données applicables aux personnes privées. Les traitements de données personnelles effectués par la Poste doivent reposer sur un motif justificatif. Pour les traitements dont il est question ici, c'est uniquement le consentement de la personne concernée qui peut être invoqué. La Poste doit donc informer de manière claire et précise ses clients sur les traitements qui sont effectués avec les données saisies et sur les buts de ces derniers. Elle doit en même temps rendre attentif à la possibilité d'interdire un traitement. Si le client interdit la mise à jour pour des tiers, seul un traitement de ses données au sein de la Poste est possible. Ce traitement peut néanmoins être effectué par une entreprise tierce pour le compte de la Poste. En sa qualité de maître du fichier, la Poste continue néanmoins à assumer la responsabilité pour l'application des dispositions en matière de protection des données.

Mat[CH]move est également offert comme prestation en ligne sur l'Internet. A des fins de démonstration, des adresses réelles ont été accessibles dans le monde entier pendant plusieurs semaines, sans qu'il ait été nécessaire d'indiquer une ancienne adresse. Ceci fut même possible dans les cas où la personne concernée avait par écrit interdit la communication des données. Une publication dans l'Internet pose des exigences supplémentaires au niveau de l'information des personnes concernées. Pour qu'un consentement soit correct, les personnes concernées doivent avoir été informées sur les risques spéciaux qui sont liés à une publication sur l'Internet.

Dans le cours de nos investigations, nous avons en outre appris que la Poste/DCL transmettait son fichier d'adresses complet (changements d'adresse) à environ une dizaine de sous-traitants qui les utilisent pour offrir de leur côté des prestations de mise à jour. Ces communications n'étaient pas portées à la connaissance des clients de la Poste et violaient ainsi la loi sur la protection des données. La communication de données fut justifiée par une intervention de la Commission de la concurrence (Comco). Il ne s'agissait pourtant que d'une enquête préliminaire de la Comco qui ne présentait aucune obligation pour la Poste de fournir des données personnelles à des tiers. Même si une telle communication était exigée pour des raisons du droit de la concurrence, les données des personnes qui ont interdit la communication de leurs données ne devraient

en aucun cas être transmises, elles devraient être traitées uniquement au sein de la Poste.

La Poste nous a assuré que les données saisies sur les formules de réexpédition ne seront dorénavant plus communiquées à des tiers. Les mises à jour pour des tiers ne seront effectuées que dans les cas où une adresse antérieure complète peut être fournie. Le client de la Poste doit cependant être informé de manière bien compréhensible sur la mise à jour et il est en droit de l'interdire. Nous avons soumis à la Poste une proposition pour une clause de consentement pouvant être intégrée dans le formulaire. La Poste a rejeté notre proposition et, en collaboration avec le Département fédéral de l'environnement, des transports, de l'énergie et de la communication, a élaboré un projet de disposition légale autorisant la mise à jour d'adresses figurant dans les fichiers de tiers.

Des problèmes liés à la protection des données sont également apparus en rapport avec deux autres prestations de service et les données saisies parallèlement à l'aide des nouveaux formulaires. A notre avis, les données saisies sur les formulaires «Demande de réexpédition temporaire» ainsi que «Courrier à garder à l'office de poste» (année de naissance, sexe, profession, etc.) dépassent largement le cadre des données qui seraient nécessaires pour fournir la prestation.

4. INTERNET et technologies de la vie privée

4.1. Respect du principe de la proportionnalité pour les programmes de démonstration sur l'Internet

Les entreprises fournissant contre paiement des informations personnelles sur l'Internet désirent faire aux intéressés une démonstration aussi réaliste que possible de leurs offres de prestations afin de pouvoir les gagner comme clients. En essayant d'atteindre ce but, il leur arrive parfois d'exagérer et de violer ainsi le principe de la proportionnalité, parfois aussi celui de l'exactitude des données.

L'Internet est une plate-forme particulièrement attrayante pour la commercialisation de divers produits, notamment aussi de données personnelles. Il arrive donc que les conditions cadre de la protection des données ne soient pas toujours respectées. Les personnes privées qui rendent accessibles des données personnelles sur l'Internet doivent disposer d'un motif justificatif, la plupart du temps sous forme du consentement de la personne concernée, obtenu après que celle-ci ait été informée en détail sur les risques.

Nous avons été forcé d'intervenir pour plusieurs prestations de services proposées dans le domaine des renseignements de crédit et de la mise à jour d'adresses, étant donné que des données personnelles avaient été rendues accessibles dans le programme de démonstration déjà sans que cela soit vraiment nécessaire.

Le programme de démonstration d'un système d'information sur la solvabilité ne doit pas pouvoir être utilisé comme annuaire d'adresses ni dévoiler des données personnelles sous quelque forme que ce soit. En particulier, il ne doit pas être possible de voir si une personne précise, indiquée par l'utilisateur Internet, est répertoriée dans un tel système d'information. Une telle opération serait en contradiction avec le principe de la proportionnalité, même si le fait de constater que la personne en question est répertoriée dans le système d'information ne permet pas à priori d'en déduire qu'elle n'est pas solvable. C'est pourquoi seules des données fictives doivent être utilisées pour le programme de démonstration. Seul le client (payant) qui demande une information sur un potentiel partenaire commercial afin de vérifier la solvabilité de ce dernier doit être en mesure d'accéder aux données personnelles.

Ceci vaut de manière analogue pour les prestations dans le domaine de la mise à jour d'adresses. Dans ce cas également, des données fictives suffisent à démontrer les performances du système. Le client ne doit obtenir une adresse mise à jour que s'il est en mesure de fournir une des anciennes adresses.

Nous avons malheureusement du constater que des données personnelles étaient accessibles dans des programmes de démonstration sur l'Internet même dans les cas où les personnes concernées avaient explicitement interdit par écrit la communication de leurs données à des tiers.

Un autre problème de protection des données est apparu dans la mesure où il arrivait dans certains cas que plusieurs adresses postales soient affichées pour une seule personne concernée. En plus du domicile actuel, le système affichait plusieurs anciennes adresses. L'utilisateur qui accédait aux données dans le but unique de se faire présenter le système ne pouvait pas savoir laquelle des adresses était l'adresse actuelle, ce qui violait donc le principe de l'exactitude des données. Comme nous l'avons mentionné précédemment, il n'est de toute façon pas permis d'utiliser des données personnelles réelles dans un programme de démonstration.

Les prestations contestées ont entre-temps été adaptées par les exploitants. Il ne fait cependant aucun doute qu'il existe d'autres prestations du même type qui ne sont pas conformes aux dispositions de la loi sur la protection des données.

4.2. Accès non autorisé à des bases de données sur l'Internet

La mise en réseau croissante a pour effet que – suite à des erreurs et négligences de la part des exploitants des systèmes – il se produit de plus en plus souvent que des banques de données qui ne devaient en aucun cas être accessible sur l'Internet ou alors uniquement pour un cercle défini d'utilisateurs autorisés deviennent accessibles au grand public.

A la fin de l'année écoulée, nous avons reçu une indication de la part d'un développeur de logiciels qu'il était possible à travers l'Internet d'accéder de manière non autorisée à plusieurs bases de données du type Microsoft SQL Server, fait que nous avons effectivement pu vérifier. Il était non seulement possible de lire ces données, mais également de modifier le contenu de tous les champs de données et même de les supprimer. Cette brèche de sécurité a été rendue possible par la négligence des exploitants de la base de données qui avaient omis de modifier le mot de passe de l'administrateur qui est prédéfini par le fournisseur du logiciel. En peu de temps, nous avons découvert par hasard plusieurs douzaines de bases de données qu'il était possible de lire et de manipuler suite à cette négligence. En plus d'un nombre de données anodines, certaines de ces bases de données contenaient également des données très sensibles telles que des liste de mots de passe et des numéros de cartes de crédit.

Même s'il faut constater qu'un utilisateur Internet non chevronné n'était pas en mesure sans autre de tirer profit de cette brèche de sécurité pour accéder de manière non autorisée à une base de données, nous somme d'avis que cette situation était grave. Nous avons donc exhorté par voie de presse les exploitants de la base de données concernée de modifier immédiatement le mot de passe de l'administrateur prédéfini par le fournisseur.

Ces derniers temps, nous avons en outre découvert plusieurs autres cas dans lesquels il était possible d'accéder par l'Internet à des données internes à une entreprise. Il suffisait dans ces cas de connaître l'adresse Internet (URL) exacte pour pouvoir avec un navigateur Web accéder directement à ces données. Dans ces cas, il s'agissait également de données sensibles, telles que des informations de paiement ou des agendas personnels. Nous avons dans tous ces cas informés les entreprises concernées afin qu'elles puissent rétablir la sécurité.

5. Commerce électronique et protection des données

5.1. Eléments clés du développement du commerce électronique

Nous aimerions souligner ci-dessous un certain nombre d'éléments jouant un rôle déterminant dans le développement du commerce électronique:

- Le commerce électronique est une opération «*one-to-one*». En d'autres termes, il repose exclusivement sur le contact personnel. Le consommateur réagira donc avec réserve s'il ne peut se protéger contre un flot de publicité et d'informations. Bon nombre d'entreprises rassemblent déjà des données personnelles sur leurs clients. Leur but: mettre sur pied des banques de données pour personnaliser leur offre. Si les consommateurs n'en sont pas informés, leur confiance s'en trouvera atteinte.

- Les autorités jouent un rôle clé dans la mise en place du cadre dans lequel le commerce électronique se déroulera. A ce propos, la protection de la sphère privée figure en première position sur la liste des priorités.

- Si l'on veut assurer à long terme le succès du commerce électronique et parvenir à une stabilisation du marché, il faut résoudre le problème de la protection efficace de la sphère privée. Un point essentiel à cet égard est le choix du droit applicable en cas de litige. Les Etats-Unis appliquent le droit du prestataire, alors que c'est le droit applicable au domicile du consommateur qui devrait l'être. C'est également l'un des aspects essentiels à l'établissement d'une relation de confiance avec l'utilisateur.

Au niveau international, il convient de mettre l'accent sur les thèmes suivants:

- Les mesures destinées à mettre l'utilisateur en confiance (notamment la protection de la sphère privée) doivent être efficaces.
- Les réglementations nationales et codes de conduite d'une part et les solutions technologiques telles la signature digitale ou les technologies modernes de protection de la vie privée (PET, privacy enhancing technologies) de l'autre doivent être complémentaires et reconnues au niveau international.
- L'OCDE doit contribuer à la concrétisation des points que nous venons d'énumérer en entretenant le dialogue avec tous les acteurs (économie, autorités, consommateurs et organisations internationales).

En Suisse, les efforts porteront plus particulièrement sur les éléments suivants:

- Les représentants suisses au sein des organisations internationales continuent à soutenir les mesures à même de mettre en confiance l'utilisateur du commerce électronique.

- Face à la difficulté de choisir entre réglementations nationales et codes de conduite, il conviendrait d'adopter une solution associant les deux modèles. Les codes de conduite doivent néanmoins protéger le consommateur au moins de façon aussi efficace que les réglementations nationales. S'ils ne déploient pas le degré d'efficacité requis, la protection du consommateur requiert impérativement une réglementation au niveau national.

- Le plan d'action qui existe déjà en Suisse à propos du commerce électronique doit être rapidement mis en pratique. Les mesures destinées à assurer la confiance du consommateur (formation, information du public, protection de la sphère privée) figurent au premier plan.

5.2. Renseignements sur l'élaboration d'une déclaration de traitement de données sur Internet

Les déclarations de traitement de données ont pour but d'informer l'utilisateur d'un site Internet du procédé utilisé par le prestataire de services pour protéger la sphère privée de ses clients. Elles constituent un pas important vers l'établissement d'une relation de confiance, à condition que la déclaration présente la rigueur nécessaire. C'est là le seul moyen, pour l'utilisateur, de décider librement s'il désire que ses données personnelles soient traitées et sous quelle forme.

Face à l'essor du commerce électronique, la protection des données personnelles revêt une importance de plus en plus grande pour l'utilisateur de prestations en ligne. Les sondages effectués sur Internet font ressortir que nombreux sont ceux qui hésitent encore à faire leurs achats par Internet parce que la confidentialité de leurs données personnelles n'est pas garantie. Pour que le commerce électronique puisse développer tout son potentiel et inspire confiance aux utilisateurs, il faut prendre dès aujourd'hui les mesures nécessaires pour protéger leur sphère privée.

Nous recommandons aux entreprises suisses qui offrent leurs prestations sur Internet de pratiquer une politique transparente en matière de traitement des données, en insérant sur leur site Web une déclaration de traitement de données.

Avant d'en entamer l'élaboration, l'entreprise devra étudier ses besoins de données, analyser sa pratique en matière de protection des données et établir des directives claires sur la manière de gérer les données personnelles recueillies. La déclaration de traitement de données sera rédigée sur la base de ces indications. Elle concordera avec la loi sur la protection des données et correspondra aux traitements de données réellement effectués.

Avant de rédiger la déclaration de traitement de données, nous incitons les prestataires à examiner les points suivants:

- Comment et à partir de quelle source (interne ou externe) les données sont-elles collectées ?
- Dans quels buts les données personnelles sont-elles collectées ?
- Dans quels buts les données personnelles sont-elles utilisées ?
- Qui est responsable du contrôle des données personnelles collectées ?
- Comment et où la sauvegarde des données personnelles a-t-elle lieu ?
- Dans quels buts des données personnelles sont-elles échangées avec des tiers ?
- Existe-t-il déjà des directives ou des prescriptions relatives à la collecte, au traitement et à la communication de ces données ?
- La personne concernée a-t-elle la possibilité de consulter ou de faire rectifier ses données ?

La déclaration devrait répondre, à l'intention de l'utilisateur, au moins aux questions suivantes:

- A quelles dispositions légales la pratique du prestataire est-elle soumise en matière de traitement des données ?
- Quelles données personnelles sont collectées et dans quels buts ?
- Quelles données personnelles sont communiquées à des tiers et dans quels buts°?
- Quels choix sont proposés à l'utilisateur quant au traitement de ses propres données ?
- Quels sont les droits (notamment droit d'accès et droit de rectification) dont dispose l'utilisateur ?
- Quel service est chargé de répondre aux questions sur le traitement de données personnelles ?
- Quelles mesures de sécurité sont appliquées pour protéger les donnés personnelles ?

Enfin, il convient de placer la déclaration sur le site de l'entreprise de telle manière qu'elle soit facilement accessible à l'utilisateur.

Voir également page 225 Générateur de l'OCDE pour la protection des données et Déclarations types et directives du conseil de l'Europe sur la protection de la sphère privée sur Internet (www.coe.fr/dataprotection).

6. Personnel

Administration fédérale

6.1. Surveillance par vidéo sur le lieu de travail: définition de la surveillance du comportement

Les systèmes de surveillance et de contrôle censés surveiller le comportement des employés sur le lieu de travail ne sont pas autorisés. Même un comportement incorrect, voire illicite, ne doit pas être contrôlé par l'employeur à l'aide de moyens techniques. En effet, l'administration de la preuve en vue de poursuivre une infraction est du ressort des autorités pénales.

Nous avons été consultés à propos du caractère licite ou illicite d'une installation de surveillance vidéo placée dans un centre de tri postal. Nous nous sommes rendus sur place et avons constaté que l'installation en question était composée de plusieurs caméras vidéo surveillant le secteur du tri manuel, ainsi que l'arrivée des camions et le hall d'entrée. Les caméras vidéos installées à l'arrivée des camions et dans le hall d'entrée surveillent les entrées et les sorties de véhicules et de personnes, ainsi que les allers et venues dans le hall d'entrée. Les caméras vidéos installées dans le secteur du tri manuel surveillent les employés d'une part au tri manuel et automatisé des lettres, d'autre part aux abords des entrées des ascenseurs et des toilettes. Les images enregistrées au tri manuel et aux abords des entrées des ascenseurs et des toilettes sont retransmises dans le bureau du responsable de la sécurité, où elles sont enregistrées en permanence, soit jour et nuit, sur cassettes. Personne n'est en principe assis en permanence devant l'écran et les enregistrements ne sont regardés en direct que de manière sporadique. Ils sont conservés pendant un mois et demi environ, puis effacés s'il n'est pas nécessaire de reconstituer un cas de vol ou si les éléments de suspicion ne sont pas confirmés. Les personnes concernées ont été informées en 1996 par une lettre, affichée au tableau du centre de tri, décrivant l'utilisation et le but du système de surveillance par vidéo. Quant aux employés arrivés ultérieurement, ils ont été mis au courant plus ou moins en détail de vive voix, par leurs propres collègues dans la plupart des cas.

Au centre de tri, la surveillance par vidéo a pour but la lutte contre les délits dit « d'insiders » (essentiellement des vols) et la détection des pertes. L'article 26 de l'ordonnance 3 relative à la loi sur le travail renferme une interdiction de surveillance du comportement. Ainsi, même un comportement indésirable, voire illicite, ne doit pas être contrôlé à l'aide de moyens techniques. L'entreprise doit choisir d'autres voies pour se protéger contre ce genre de comportements. Les directives de l'Organisation internationale du travail à Genève interdisent également la mise en œuvre de mesures techniques et organisationnelles destinées à surveiller le comportement et les mouvements des employés. Alors que le contrôle de la performance et de la sécurité sont licites, tant le droit suisse que le droit international excluent expressément la surveillance du comportement. Le droit suisse est plus strict que les directives internationales, qui parlent la plupart du temps de surveillance permanente, car il entend aussi par surveillance du comportement un contrôle non permanent du comportement. La surveillance du comportement et de la prestation sont souvent étroitement liées et, dans bien des cas, il est difficile ou même impossible de délimiter avec précision la surveillance de la prestation, de la sécurité ou du comportement (exemple: l'enregistrement précis du nombre de frappes avec indication exacte de la répartition dans le temps tout au long de la journée permettrait de tirer des conclusions sur le comportement). Dans le cas qui nous occupe ici, il n'est question ni de surveillance de la prestation, ni de surveillance de la sécurité.

En effet, la direction du centre de tri ne procédant pas à une évaluation systématique des enregistrements, on ne peut parler de surveillance des prestations. Quant à la surveillance de la sécurité, il ne peut en être question que dans le cadre du contrôle de la gestion de la production ou du contrôle à l'égard de tierces personnes (par ex. personnes qui viennent de l'extérieur). Conformément aux dispositions en vigueur et à leur stricte interprétation et application, la surveillance des vols par l'employeur à l'encontre de ses propres employés n'est pas considérée comme contrôle de la sécurité, mais comme contrôle illicite du comportement. Cela est dû essentiellement au fait qu'il incombe aux autorités pénales et non à l'employeur d'ordonner les relevés et mesures de conservation des preuves (par ex. de surveillance par vidéo); en effet, le vol est un acte à caractère pénal et la surveillance du comportement peut porter gravement atteinte à la personnalité. Exceptionnellement, l'employeur peut relever et conserver lui-même des preuves en procédant à des enregistrements vidéo lorsque l'attente d'une intervention des autorités compétentes comporte un risque concret et sérieux de perte ou de destruction d'un moyen de preuve. Dans ce cas, il demeure tenu de demander ultérieurement l'intervention de l'autorité compétente. Par ailleurs, il doit y avoir un soupçon concret d'infraction contre une personne déterminée. Lorsqu'il n'y a pas de danger de perte ou de destruction des preuves, les relevés de preuves par l'employeur peuvent non seulement être considérés comme moyen de preuve illicite dans le cadre de la procédure pénale, mais aussi avoir des conséquences en droit pénal et civil.

Au centre de tri des lettres, la surveillance par caméras vidéo touche en même temps non pas certaines personnes seulement, mais un grand nombre de personnes (en majorité innocentes). Celles-ci ne sont pas surveillées en raison d'un soupçon concret, mais de manière préventive et sans recours préalable à l'autorité compétente. En outre, circonstance aggravante, la surveillance n'est pas limitée dans le temps, mais couvre l'intégralité du temps de travail pour au moins une partie des employés. Par ailleurs, le fait que cette surveillance n'ait pas fait baisser le nombre des vols annoncés, mais qu'au contraire ils aient augmenté, parle en défaveur de ce système de surveillance par vidéo. Il convient donc également de contester l'efficacité du système en tant que moyen d'intimidation. Conformément à la loi sur la protection des données, les données personnelles ne peuvent être traitées que dans le but qui est indiqué lors de leur collecte, qui ressort clairement des circonstances et qui est prévu par une loi. Cela exclut une collecte de données effectuée à des fins préventives. Néanmoins, c'est l'ensemble de la politique de surveillance du centre de tri qui est à mettre en doute; ainsi, dans d'autres secteurs « sensibles » du bâtiment (par ex. celui des paquets), il n'y a aucune surveillance. L'installation de surveillance par vidéo pèche également par son manque de proportionnalité. En effet, selon le principe de la proportionnalité, l'employeur ne peut traiter des données sur l'employé que si elles concernent son aptitude à remplir son emploi ou sont nécessaires à l'exécution de son contrat de travail. Comme la statistique des vols nous a permis de le constater, ce système de surveillance n'a pas eu un effet d'intimidation et n'a pas permis de découvrir les auteurs des vols. Selon les indications fournies par les personnes concernées, le contrôle constant dans le secteur du tri manuel provoque une pression psychologique dont l'une des causes, et non la moindre, est le manque d'information sur la portée et le but de cette surveillance. Un tel contrôle est en contradiction avec l'esprit de l'ordonnance 3 sur le travail, à savoir la prévention en matière de santé et la protection de la personnalité. Selon le principe de la bonne foi, les personnes concernées doivent être informées de la présence de caméras. Cela ne signifie pas seulement que les caméras vidéo doivent être installées de manière visible pour les personnes concernées, mais aussi que celles-ci soient informées expressément et par écrit (par ex. lors de l'embauche par une clause dans le contrat de travail) de la portée et du but du système de surveillance.

Ces considérations valent également pour le contrôle des entrées des ascenseurs et des toilettes, qui n'est pas à considérer comme séparé, mais au contraire comme faisant partie intégrante d'un seul et même système de surveillance. Ce système autorise une surveillance intégrale du comportement, en ce sens que les personnes concernées ne sont pas observées seulement pendant le travail effectif, mais aussi durant les moments improductifs, comme par exemple l'entrée et la sortie des toilettes. Par ailleurs, la surveillance des entrées d'ascenseur ne concerne pas seulement les employés du secteur du tri manuel, mais aussi les entrées et sorties d'autres employés qui travaillent aux autres étages du

bâtiment. Dans le dernier cas également, il s'agit d'une surveillance du comportement au sens de l'ordonnance 3 sur le travail. La surveillance par vidéo du tri manuel ainsi qu'aux abords des entrées des ascenseurs et des toilettes constitue donc une violation de la personnalité d'un grand nombre de personnes. Même si les employés concernés donnaient leur consentement exprès à l'installation d'un système de surveillance par vidéo, on ne pourrait déroger aux prescriptions contraignantes en matière de protection de la personnalité imposées par le droit des obligations.
En revanche, la surveillance par vidéo de l'entrée des camions et du hall d'entrée a pour but de contrôler les entrées et les départs de véhicules et de personnes dans le secteur d'arrivée des camions, ainsi que les allers et venues de personnes dans le hall d'entrée. Contrairement à la surveillance du comportement des employés, un contrôle de la sécurité orienté vers l'extérieur est permis (en d'autres termes, le contrôle des entrées non autorisées) dans la mesure où les employés eux-mêmes ne sont pas filmés par les caméras ou à la rigueur ne le sont qu'exceptionnellement.

Etant donné la situation juridique, nous avons demandé au centre de tri d'éliminer le système de surveillance par vidéo dans le secteur du tri manuel, ainsi qu'aux abords des entrées des ascenseurs et des toilettes, et de garantir la sécurité interne à l'aide d'autres mesures, par exemple en renforçant la présence de supérieurs ou de personnes chargées de la sécurité.

6.2. Législation sur les fonctionnaires et BV-PLUS

Les exigences posées par le droit de la protection des données à propos de la base légale requise pour le traitement des donnés relatives au personnel de la Confédération n'ont pas été encore transposées dans les faits. De même, la décision formelle du Département des finances sur la répartition des compétences entre l'Office fédéral du personnel et les autres services du personnel n'a pas encore été prise.

Comme nous l'avons déjà mentionné dans le dernier Rapport d'activités (6ème Rapport d'activités 1998/99, p. 252) à propos de la création de la nouvelle loi sur le personnel de la Confédération, les exigences posées par la LPD à propos de la base légale requise pour le traitement des données concernant le personnel de la Confédération n'ont pas été suffisamment concrétisées. Une solution de compromis a été ultérieurement élaborée avec le Département fédéral des finances dans le cadre de la procédure de corapport. Cette solution de compromis prévoit les exigences minimales que doit remplir une base légale formelle pour le traitement de données sensibles, en particulier celles concernant le personnel de la Confédération, la procédure d'appel des données ainsi que la communication de données à des tiers. Le traitement et la communication de données médi-

cales concernant le personnel de la Confédération ont été également réglementés dans une disposition spéciale. Il a été convenu que cette solution de compromis devrait être prise en compte non pas dans le cadre de l'adaptation de la loi sur le statut des fonctionnaires conformément à l'art. 38 LPD, mais à l'occasion de la création de la nouvelle loi sur le personnel de la Confédération. Cette nouvelle loi fait toujours défaut.
De même, la décision formelle du Département fédéral des finances relative à la séparation des compétences entre l'Office fédéral du personnel et les autres services du personnel de l'administration fédérale n'a pas encore été rendue.

6.3. Protection des données dans les offices régionaux de placement (ORP)

A la suite des incidents survenus en 1997 en relation avec la publication sur Internet de données concernant les chômeurs, l'office fédéral compétent a pris une série de mesures afin de mieux garantir la protection des données dans les ORP.

En 1997, les données concernant des chômeurs, traitées dans le système d'information sur le marché du travail « PLASTA », ont été accessibles dans le monde entier sur Internet durant une courte période. Nous avions alors constaté le caractère illicite du traitement, par les ORP, de certaines données personnelles concernant des chômeurs (cf. 5e Rapport d'activités 1997/98, p. 173). Suite à notre intervention, l'office fédéral compétent (aujourd'hui le Secrétariat d'Etat à l'économie) a pris diverses mesures pour améliorer la protection des données dans les ORP. Entre autres, une circulaire a été élaborée à propos de la protection des données lors de l'exécution de la loi sur l'assurance-chômage et de la loi sur le service de l'emploi et la location de services. Cette circulaire établit en particulier les catégories de données qui ne doivent pas être saisies ou uniquement au cas par cas, si le besoin est prouvé. Ces catégories de données correspondent en gros aux données sensibles selon la LPD. Le Secrétariat d'Etat à l'économie a également organisé un stage de formation pour les responsables des ORP. Ce stage a essentiellement pour but d'expliquer la signification de la protection des données et de la circulaire pour que cette dernière puisse être appliquée plus efficacement. Sous la conduite d'un préposé cantonal à la protection des données, nous avons rendu visite à un ORP et avons constaté dans quelle mesure la circulaire et les dispositions de protection des données étaient appliqués. Nous nous rendrons prochainement dans d'autres ORP.

Secteur privé

6.4. Aide-mémoire relatif à la protection des données lors de l'utilisation du téléphone sur le lieu de travail

Un groupe de travail composé de préposés cantonaux et du préposé fédéral à la protection des données ont réglementé, dans un aide-mémoire, la surveillance de l'utilisation du téléphone sur le lieu de travail. Cet ouvrage souligne essentiellement l'interdiction des écoutes téléphoniques et des enregistrements de conversations privées; il précise également les conditions que doit remplir un enregistrement licite de données relatives aux appels privés. Cet aide-mémoire aborde enfin la surveillance des appels téléphoniques professionnels sur le lieu de travail, ainsi que les caractéristiques spécifiques auxquelles doivent répondre les installations téléphoniques (cf. annexe p. 241).

7. Assurances

Assurances sociales

7.1. Adaptation de la législation sur les assurances sociales à la loi sur la protection des données

Les textes législatifs sur les assurances sociales ont été adaptés à la législation sur la protection des données. Sur certains points, des divergences demeurent néanmoins entre l'Office fédéral des assurances sociales (OFAS) et le Préposé fédéral à la protection des données (PFPD). Le message relatif à cette harmonisation des textes de loi a enfin été publié le 8 février 2000.

La législation sur les assurances sociales est tenue de répondre aux exigences de la loi sur la protection des données d'ici à fin 2000 (cf. également 6ème Rapport d'activités 1998/99, p. 260/261). La révision de ces textes a pour but de créer les bases légales formelles requises pour les fichiers déjà constitués qui contiennent des données sensibles ou des profils de la personnalité.
Dans le cadre de la consultation des offices, le PFPD s'est prononcé à plusieurs reprises sur le « Message concernant l'adaptation et l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales ». Néanmoins, l'OFAS et le PFPD n'étant pas parvenu à un accord dans tous les domaines, une procédure de corapport a été menée. En substance, le PFPD reproche aux normes leur insuffisance du point de vue du principe de la légalité.

Nous avons par exemple constaté que les bases légales régissant les activités des diverses autorités de surveillance sont vagues et imprécises. Par ailleurs, l'application par analogie de la législation sur l'AVS à d'autres textes législatifs sur les assurances sociales est, dans la pratique, une source de problèmes. En effet, elle ne fournit la transparence nécessaire ni aux autorités, ni aux personnes concernées. De plus, on ne peut pas tout simplement transposer dans d'autres domaines des assurances sociales les dispositions sur la protection des données relatives à l'AVS. Du point de vue juridique, le traitement de données personnelles dans le domaine de l'AI par exemple diffère totalement du traitement de données personnelles dans le domaine de l'AVS. L'assurance-invalidité implique par ailleurs le traitement de données médicales sensibles (par exemple les expertises psychiatriques), lequel traitement nécessite donc une base légale au sens formel.
En outre, le projet d'harmonisation des différents textes législatifs sur les assurances sociales est en contradiction partielle avec l'objectif initial de la présente révision.
D'une part, nous regrettons que, dans certains domaines, cette harmonisation se fasse au détriment de la personne assurée. Il s'agit ici en particulier de la transmission de données personnelles (exceptions à l'obligation de garder le secret), que l'on envisage d'élargir. Contrairement au message, le PFPD est donc d'avis que les innovations prévues justifient une procédure de consultation.
D'autre part, du fait justement des mesures d'harmonisation, la réglementation des traitements de données dans les différentes lois est insuffisante et imprécise. Les données ne doivent pas être traitées de la même manière dans toutes les assurances sociales. C'est un point dont les différents projets de loi n'ont pas suffisamment tenu compte.

7.2. Fonds des caisses de pension: recherche des ayants droit

Récemment créée, la Centrale du 2e Pilier a pour mission de rendre les « avoirs oubliés » des caisses de pension à leurs ayants droit. Or la procédure prévue par la loi sur le libre passage (LFLP) ne permet pas de les retrouver tous. On cherche donc actuellement à rassembler les adresses manquantes par d'autres voies. L'introduction éventuelle de traitements de données supplémentaires nécessitera néanmoins l'adaptation des bases légales.

C'est un fait désormais avéré, un certain nombre d'employés n'ont pas fait valoir leurs prétentions au titre du 2e pilier auprès de leurs organismes de prévoyance. Dans la plupart des cas, ces « avoirs oubliés » sont probablement des comptes d'anciens saisonniers et autres personnes ayant bénéficié d'un permis à

l'année, qui ont travaillé en Suisse durant les années 70 et 80 (cf. également 6ème Rapport d'activités 1998/99, p. 261).
La loi révisée sur le libre passage est entrée en vigueur le 1er mai 1999. Cette révision a entre autres permis de mettre sur pied la Centrale du 2e Pilier, laquelle est rattachée au Fonds de garantie. Cette centrale sert d'intermédiaire entre les organismes de prévoyance, les organismes qui gèrent des comptes ou des polices de libre passage, et les assurés.
Par ailleurs, la loi fédérale sur le libre passage prévoit que la Centrale du 2e Pilier devra passer par la Centrale de compensation (CC) de l'AVS pour trouver les adresses manquantes. Néanmoins, la Centrale du 2e Pilier a signalé au PFPD que la CC n'était pas en mesure de retrouver tous les ayants droit. A son avis, cette recherche doit se faire aussi par d'autres voies, en coopération avec les différents Etats où résident désormais ces personnes. La CC précise également que la situation particulière prévalant dans chaque Etat devait être suffisamment prise en considération.

Actuellement, il n'existe pas de base légale régissant les autres traitements de données, notamment la communication de données personnelles par la Centrale du 2e Pilier à des services étrangers. La Centrale du 2e Pilier devant être considérée comme un organe fédéral au sens de la LPD, les traitements de données qu'elle effectue nécessitent une base légale. Il convient également de rappeler dans ce contexte que la Centrale du 2e Pilier, qui est rattachée au Fonds de garantie, est soumise à l'obligation légale de garder le secret. Les exceptions à cette obligation ou la communication de données personnelles à des tiers requièrent aussi une base légale.
Nous avons donc proposé à la Centrale du 2e Pilier et à l'OFAS de combler les lacunes légales par des traités. Les traités constituent une base légale suffisante et permettent de tenir compte des particularités des différents pays (notamment pour ce qui est de l'Italie et de l'Espagne). Par ailleurs, les traités bilatéraux (et les compléments éventuels aux conventions signées jusqu'ici) peuvent assez rapidement entrer en application.

7.3. Analyse des procédures dans le domaine des assurances sociales

De l'avis du PFPD, l'analyse des procédures est une méthode efficace pour contrôler si les traitements de données sont conformes à la loi. En effet, elle crée la transparence nécessaire au niveau du fonctionnement interne des autorités en charge des assurances sociales. Son efficacité est d'ailleurs de plus en plus souvent reconnue dans d'autres domaines.

Dans le domaine des assurances sociales, un certain nombre de questions reviennent régulièrement. En partie, cela tient au fait que les procédures internes violent la loi sur la protection des données (cf. également le 6ème Rapport d'activités 1998/99, p. 263). Il convient donc de remédier au manque de transparence de ces procédures internes et de les modifier en conséquence.
Un office régional de placement a déjà fait l'objet d'une analyse des procédures. Actuellement, en collaboration avec l'OFAS, nous examinons le fonctionnement interne d'un service en charge de l'AI. Dans une première phase, nous étudions les dossiers de ce service. Puis nous recherchons d'autres informations éventuellement nécessaires et, enfin, nous définissons les objectifs et l'ampleur de l'analyse. Par la suite, nous interrogerons les personnes sur place et, en dernier lieu, nous établirons un rapport final. Les procédures internes du service en question devront être modifiées en fonction des résultats de l'analyse. Ultérieurement, il conviendra d'adapter également les circulaires et les bases légales.

Dans le domaine de l'assurance-maladie, quelques caisses sont aussi en train de soumettre leurs procédures internes à une analyse. Dans cet esprit, l'OFAS a également renforcé sa surveillance sur les assureurs et analyse les procédures auprès de différents assureurs. Nous saluons le fait que l'OFAS, dans le cadre de son activité de surveillance, entende également contrôler le respect des principes de la protection des données.

7.4. Commission d'experts sur la protection de la personnalité dans l'assurance-maladie et l'assurance-accidents sociales et privées

Le rapport de la Commission d'experts sur la protection de la personnalité dans l'assurance-maladie et l'assurance-accidents sociales et privées est en cours d'élaboration. Les travaux de la commission accusent un certain retard, pour diverses raisons.

La commission aurait dû achever ses travaux fin 1999. Les questions à traiter ont été exposées en détail dans le dernier Rapport d'activités (cf. 6ème Rapport d'activités 1998/99, p. 264).
Les nombreux thèmes abordés sont complexes. Dans le secteur de la santé en particulier, le but des traitements de données n'apparaît pas toujours très clairement. Il est par exemple difficile de déterminer les données personnelles dont les caisses-maladie ont besoin pour vérifier le caractère économique des prestations. En Suisse, nous ne disposons pratiquement d'aucun savoir-faire scientifique à ce propos, ce qui ne facilite pas les choses. Néanmoins, il convient d'abandonner le code CIM-10 qui n'est ni utile, ni approprié (cf. éga-

lement p. 175). Il convient dans tous les cas de respecter le principe de la proportionnalité posé par le droit de la protection des données.
Dans bien des cas, le savoir et l'expérience des membres de la commission ne suffisent pas pour résoudre les problèmes posés. La discussion demeure alors trop théorique et superficielle. On risque par ailleurs de ne pas estimer à leur juste valeur les problèmes qui se posent. Il serait judicieux de faire analyser les différentes tâches avec plus de précision. Les travaux de la commission s'en trouveraient ainsi prolongés.
Par ailleurs, dans le domaine de la santé tout particulièrement, on constate un durcissement des « fronts ». Il sera donc difficile de parvenir à des solutions favorables à la protection des données et surtout de les mettre en pratique.
Le rapport de la commission devrait être achevé fin juin 2000.

7.5. Tribunal fédéral: la protection des données concerne aussi les documents internes

Dans le domaine de l'assurance-accidents, on faisait jusqu'ici la différence entre les documents internes et les documents externes. Contrairement aux documents externes, les assurés ne pouvaient pas avoir accès aux documents internes. Dans un récent arrêt, le Tribunal fédéral a estimé que l'accès aux documents internes ne pouvait, en principe, pas être refusé.

La distinction entre documents internes et externes n'est pas seulement faite dans le domaine de l'assurance-accidents obligatoire. Elle l'est également dans presque tout les secteurs des assurances sociales. Les documents externes sont considérés comme des preuves et peuvent être communiqués aux personnes concernées. Par contre, l'accès aux documents internes, censés être destinés uniquement à un usage administratif interne, leur était jusqu'ici refusé. Le préposé fédéral à la protection des données (PFPD) a toujours estimé que cette distinction généralement faite entre documents internes et externes était contraire au droit (cf. 5ème Rapport d'activités 1997/98, p. 190/191).
Le Tribunal fédéral a rendu un arrêt dans lequel il déclare cette distinction générale incompatible avec la loi sur la protection des données (cf. jugement 1A.218/1998 du 1.9.99 – uniquement des extraits de ce jugement seront publiés). En effet, le droit d'accès s'étend à toutes les données sur une personne qui sont contenues dans un fichier (cf. art. 8 LPD). Les documents internes relatifs à cette personne en font également partie. C'est pour elle la seule manière de faire valoir tous ses droits en matière de protection des données.
Le Tribunal fédéral relève par ailleurs que l'accès à des documents pourrait gêner la formation d'une opinion au niveau interne. Dans ce cas, une certaine restriction serait à ses yeux justifiée. Il estime néanmoins que la limitation du

droit d'accès devrait être limitée au strict nécessaire dans le temps et sur le fond: dans le temps, l'accès ne devrait être restreint qu'au niveau de la première instance; sur le fond, le renseignement demandé pourrait être refusé uniquement aussi longtemps que l'exige la formation de l'opinion au niveau interne.
A ce propos, le PFPD désire toutefois souligner que les exceptions au droit d'accès sont réglementées de manière exhaustive dans la loi sur la protection des données (cf. art. 9 LPD). Il convient d'en tenir compte dans chaque cas.
Nous avons donc à nouveau prié l'OFAS de modifier la pratique actuelle et d'adapter en conséquence les diverses circulaires utilisées dans le domaine des assurances sociales.

7.6. Cas concernant le domaine de l'AI

- Preuve d'une atteinte à la santé dans les centres de désintoxication

L'Office fédéral des assurances sociales (OFAS) a entre autres besoin de données médicales avant de décider si un centre de désintoxication peut bénéficier de subventions de l'AI. Cette démarche nécessite néanmoins une base légale au sens formel. Bien que nous l'ayons signalé à plusieurs reprises à l'OFAS, les bases légales requises manquent encore.

Les centres de désintoxication doivent répondre à certaines conditions pour pouvoir bénéficier de subventions de l'assurance-invalidité de la part de l'OFAS. Ils sont notamment tenus de prouver que les résidants présentent une atteinte à la santé à prendre en considération au sens de la législation sur l'assurance-invalidité (cf. également 6ème Rapport d'activités 1998/99, p. 266/267).
L'OFAS estime que pour établir cette preuve, il faut disposer de données médicales. A notre avis, il conviendrait d'examiner si ces données sont réellement nécessaires dans tous les cas. Une chose est néanmoins sûre, la collecte de données personnelles sensibles requiert des bases légales au sens formel. Jusqu'ici, l'OFAS a fondé sa pratique en matière de subvention sur la jurisprudence du Tribunal fédéral des assurances et sur des directives internes. Cela n'est néanmoins pas suffisant.
Le PFPD a donc signalé à plusieurs reprises à l'OFAS que ces bases légales étaient insuffisantes. Les projets ultérieurs de révision de l'ordonnance sur l'assurance-invalidité ne contenaient également aucune disposition à ce sujet. En outre, il est difficile de savoir si l'OFAS utilise éventuellement ces données personnelles à d'autres fins.
Par ailleurs, toute collecte de données doit être transparente. Valable en particulier pour la collecte de données sensibles, cette obligation figure expressé-

ment dans la loi sur la protection des données. Or, bien qu'il l'ait promis, l'OFAS n'a toujours pas informé les assurés par une notice. Enfin, l'OFAS, en sa qualité d'organe fédéral, n'a pas encore annoncé auprès de nos services les différents fichiers concernant les centres de désintoxication.

- Formulaires et principe de proportionnalité

Des formulaires préimprimés sont utilisés dans le domaine de l'assurance-invalidité. La pratique montre que ces formulaires violent souvent les dispositions de protection des données.

Plus de 400 différents formulaires sont utilisés dans le domaine de l'AI. Certes, une telle profusion favorise peut-être le traitement rapide des dossiers. Force est néanmoins de constater que bon nombre de formulaires violent les dispositions de protection des données.
Certains enfreignent le principe de la proportionnalité. Par exemple, le formulaire d'annonce pour la perception de prestations de l'assurance-invalidité ne doit pas nécessairement demander la totalité d'un jugement de divorce, alors que seul le dispositif du jugement suffit. Autre exemple: jusqu'ici, le médecin avait la possibilité d'être informé de la décision des autorités en charge de l'AI par le formulaire « Rapport médical ». Cette possibilité est également superflue.
Dans le cadre de la procédure d'annonce, certains services en charge de l'AI demandent aussi des procurations leur permettant de recueillir des renseignements auprès de divers services. Cette procuration n'est pas seulement disproportionnée dans sa portée, elle manque également de transparence pour l'assuré. Elle prévoit en particulier de libérer les médecins du secret médical. Or les autorisations qui habilitent le médecin à répondre à toute question sur l'état de santé d'un assuré vont trop loin. Ce sont des « procurations générales » qui, du point de vue de la protection des données, sont à considérer comme nulles.

Les formulaires utilisés dans le domaine de l'AI doivent donc être examinés sous l'angle de leur conformité avec la protection des données. Cet examen aura probablement lieu dans le cadre du projet d'analyse des procédures (cf p. 167, Analyse des procédures dans le domaine des assurances sociales).

- Communication de données personnelles aux MEDAS par les services en charge de l'AI

Les services en charge de l'assurance-invalidité commandent des expertises auprès des MEDAS (services d'expertise médicale). A cette occasion, il arrive souvent que des dos-

siers originaux soient transmis dans leur intégralité aux services d'expertise médicale. Cette manière de procéder est incompatible avec le principe de la proportionnalité.

Les préposés cantonaux à la protection des données ont pour mission de surveiller que les organes cantonaux appliquent correctement les dispositions législatives de la protection des données. Nous avons été informés qu'un service de l'AI – qui fait donc partie des autorités cantonales – avait transmis à plusieurs reprises des dossiers dans leur intégralité aux MEDAS dans le cadre d'expertises médicales. L'OFAS est l'autorité de surveillance des services de l'AI.

Une rencontre a eu lieu entre les représentants des institutions susmentionnées et le PFPD. Les représentants du service AI en question et des MEDAS ont avancé que les expertises devraient toujours être documentées de manière exhaustive. Il convient néanmoins de préciser que, du point de vue de la protection des données, le principe de la proportionnalité vaut pour tout traitement de données. La nécessité de communiquer des données aux MEDAS doit être examinée dans chaque cas. Les données telles que les déclarations d'impôts, les extraits du compte AVS, la correspondance relative aux recours introduits contre des décisions ne devraient être requises que dans des cas extrêmement rares. Les services en charge de l'AI sont donc tenus d'adapter en conséquence leur organisation interne.

7.7. Les assurances sociales et les rapports de sortie

Les assurances sociales demandent aux hôpitaux des rapports de sortie complets. En général, ces rapports contiennent des renseignements qui ne sont ni appropriés, ni nécessaires au but en question. Dans ce cas, les assurances sociales ne sont pas habilitées à recevoir des rapports de sortie (violation du principe de la proportionnalité).

De plus en plus souvent, les hôpitaux refusent à juste titre de transmettre des rapports de sortie complets aux assurances sociales. En effet, ces rapports ont essentiellement pour but d'informer, dans la mesure du nécessaire, le médecin qui reprendra le cas. Ils ne sont pas destinés aux assureurs. D'une part, ils contiennent de nombreux renseignements et d'autre part, les données qu'ils renferment ne sont fréquemment pas nécessaires aux assurances sociales pour remplir leur devoir légal. Il convient donc d'examiner dans chaque cas les données personnelles pouvant être transmises aux assureurs.
Les services de l'AI par exemple doivent examiner si et dans quelle mesure un assuré est capable de travailler. Les assurances-accidents obligatoires doivent

déterminer si un cas d'accident est véritablement ou non un accident au sens où l'entend la loi. Il est inutile de disposer pour cela de dossiers de sortie complets. De même, les assurances-maladie obligatoires ne sont habilitées à se procurer que les données prévues par la LAMal. Elles ont en particulier tendance à demander systématiquement les dossiers de sortie (cf. également p. 177). Si les hôpitaux ne livrent pas les dossiers demandés, ils risquent de ne pas obtenir le paiement de leurs factures par les caisses-maladie. Ces procédés sont inacceptables. Le PFPD va mener d'autres enquêtes et prendra en temps voulu les mesures nécessaires.
Mentionnons enfin le fait que le principe de la proportionnalité vaut également pour les assureurs privés. Là aussi, il n'est ni nécessaire, ni approprié de fournir des dossiers de sortie complets.

7.8. Echange verbal d'informations entre la SUVA et les services de l'AI

La collaboration entre la SUVA et l'assurance-invalidité consiste dans certains cas en un échange verbal d'informations. Cette collaboration est régie par une convention. Le PFPD examine actuellement si cette convention est conforme à la protection des données.

En 1998, la SUVA et l'assurance-invalidité ont passé une convention réglementant la collaboration applicable aux cas d'invalidité. Cette convention a pour but d'accélérer la réhabilitation et d'harmoniser le degré d'invalidité en cas de suites dues uniquement à un accident (chiffre 1 de la convention).
Néanmoins, cette convention contient des dispositions problématiques, à savoir celles qui ne prévoient cette harmonisation que de vive voix. Ainsi, l'accord entre la SUVA et l'AI doit se faire « le plus rapidement possible verbalement » lorsque le degré d'invalidité de l'AI diffère (chiffre 4.3.3. de la convention). Les réglementations de ce type sont insuffisantes si l'assuré n'en est pas informé. En effet, tout traitement de données doit être effectué de manière perceptible pour ce dernier. La loi sur la protection des données le mentionne expressément pour la collecte de données sensibles et l'établissement de profils de la personnalité.
L'échange de dossiers entre la SUVA et les services de l'AI semble également problématique. Ainsi, la SUVA et les services de l'AI devraient se transmettre mutuellement des copies de rapports d'inspection, de rapports médicaux, etc. (chiffre 5.2. de la convention). Il convient d'examiner si cet échange de dossiers est permis. Il est probable que cette disposition viole tout particulièrement le principe de la proportionnalité. Le PFPD examine actuellement la convention sous l'angle de la protection des données.

Assurances privées

7.9. Lutte contre l'abus en matière d'assurance - Système central d'information (ZIS)

Le système central d'information (ZIS) a pour but de mieux protéger les compagnies d'assurances des manœuvres frauduleuses. Son règlement est en cours de remaniement. Le projet actuel n'est pas satisfaisant du point de vue de la protection des données, en particulier pour ce qui est de la transparence pour les assurés.

L'Association suisse des assurances (ASA) a mis sur pied un service chargé de lutter contre les abus en matière d'assurances, le ZIS. Ce service gère un fichier, enregistré chez nous, sur les procédures pénales et civiles pendantes et closes. Son règlement ainsi que le formulaire de déclaration sont en cours de remaniement auprès de l'ASA (cf. 6ème Rapport d'activités 1998/99, p. 274/275).
Il convient tout d'abord de souligner que le ZIS est placé sous la responsabilité de l'ASA et des compagnies d'assurance. Le fait que des institutions privées gèrent, parallèlement à l'Etat, un fichier comparable au casier judiciaire crée une situation délicate; en outre, ce fichier contient des données sensibles. Il est donc d'autant plus important de respecter les principes posés par la protection des données.

Le règlement du ZIS a été remanié et adapté à divers égards. Un point demeure néanmoins insatisfaisant: le manque de transparence du traitement des données pour les personnes concernées. Les compagnies d'assurance gèrent aussi des fichiers contenant des données sensibles et transmettent aussi ces données au ZIS. Tout comme le ZIS, elles sont donc tenues d'annoncer les fichiers auprès du PFPD (cf. art. 11, 3^{e} al. LPD). L'annonce du fichier au PFPD devrait créer la transparence nécessaire pour les personnes concernées.
Or, dans la pratique, cette annonce n'apporte pas la transparence souhaitée. La plupart des citoyens ne sont pas informés du registre des fichiers ou le sont mal. Nous avons donc suggéré aux compagnies d'assurance d'informer directement les personnes concernées de l'existence du ZIS, par exemple en remettant une notice au preneur d'assurance au cours de la procédure d'affiliation. Il serait en outre souhaitable que la personne concernée soit automatiquement informée qu'elle figure dans le ZIS. C'est d'autant plus important que les motifs d'un éventuel refus d'affiliation ne sont en général pas communiqués aux personnes concernées.
Par ailleurs, il est essentiel que l'exactitude et l'actualité des données soient toujours garanties. Si tel n'était pas le cas, des problèmes pourrait surgir à propos de la présomption d'innocence. Les formulaires d'annonce que les assurances doivent remplir et transmettre au ZIS doivent également être conçus dans ce sens.

L'ASA a soumis nos propositions à ses membres et reprendra contact avec nous.

8. Santé

8.1. Projet de certificat de protection des données du Concordat des assureurs-maladie suisses

Désireux de permettre aux caisses-maladie de traiter systématiquement le CIM-10 réduit à trois positions, le CAMS y met une exigence: l'obtention préalable, par les caisses intéressées, d'un certificat attestant que lesdites caisses traitent les informations concernant les assurés conformément aux exigences de la protection des données. Nous avons salué le développement de ce projet de certification. Il doit cependant être dissocié de la problématique du CIM-10. Nous n'avons ainsi pas accepté la proposition de joindre le recours au CIM-10 en échange de garanties de protection des données.

Dans nos précédents rapports d'activités, nous avons souligné que la communication systématique du diagnostic aux assurances-maladie est contraire à l'article 42, 3e et 4e alinéas, de la loi fédérale sur l'assurance-maladie (LAMal; 3e Rapport d'activités 1995/96 p. 172, 4e Rapport d'activités 1996/97, p. 176). La communication systématique des codes de la Classification Internationale des Maladies, traumatismes et causes de décès (CIM; CIM-10 en cas d'hospitalisation) est en effet non seulement illégale, mais également contraire au principe de proportionnalité. Elle n'est ni nécessaire ni appropriée aux besoins des caisses-maladie (5ème Rapport d'activités 1997/98, p. 232).

Certaines caisses-maladie ont investi des sommes considérables pour adapter leur informatique au CIM-10. Elles se refusent dès lors à rechercher des solutions conformes à la LAMal et répondant mieux à leurs besoins. En septembre 1999, elles nous ont cependant proposé, par le biais du Concordat des assureurs-maladie suisses (CAMS), une solution intermédiaire: la possibilité de ne communiquer systématiquement qu'une version du CIM-10 réduite à trois positions. En outre, seules les caisses-maladie dotées d'un certificat de protection des données seraient autorisées à traiter systématiquement ces codes. Ce projet de certificat est assorti d'un projet de réglementation en matière de protection des données, ainsi que d'un projet de clauses contractuelles relatives à la communication des trois positions du CIM-10 entre les fédérations d'assureurs et les hôpitaux. Ce projet de certificat prévoit en particulier de soumettre à un audit le respect des prescriptions légales de protection des don-

nées par les caisses-maladie, sous les angles juridique, organisationnel et technique.

Nous sommes favorables au développement du projet de certificat du CAMS. Il s'agit en effet d'un instrument adéquat qui permettra aux caisses-maladie de remplir leurs obligations légales. Nous avons également souligné que les caisses ont leur propre intérêt à intégrer la protection des données dans leur travail quotidien. En effet, une telle intégration aura des conséquences positives sur leur image notamment à l'égard des assurés qui sont devenus plus sensibles au respect de la protection des données. Elle assurera également des prestations de qualité et permettra une meilleure évaluation des risques et des mesures à prendre pour y pallier. Enfin, elle générera des économies par le recours à des analyses de processus qui permettront de rationaliser le travail.

Nous avons examiné la procédure de certification indépendamment du CIM-10. Nous ne voulons en effet pas faire de l'obtention dudit certificat une condition préalable autorisant la caisse-maladie "certifiée" à traiter systématiquement des extraits de codes CIM-10, dont ni la nécessité, ni l'adéquation n'ont jusque là été démontrées.

L'introduction d'une procédure de certification est une tâche de longue haleine, compliquée par la variété considérable des structures et de l'organisation des caisses. Elle impliquera le moment venu pour certaines d'entre elles des changements radicaux dans ladite organisation et dans la manière de traiter les dossiers des assurés. La certification doit être effectuée par une instance neutre, extérieure aux assurances-maladie. Elle ne peut cependant être faite par le préposé, car la LPD ne lui donne pas de compétences de décision. Il serait par contre souhaitable d'y associer les représentants des patients et des assurés.

Dans le cadre de la procédure de certification, les spécificités propres aux divers domaines d'assurance devront être prises en considération. En effet, selon qu'une caisse agit à titre d'assureur privé ou social, elle n'est pas soumise aux mêmes législations, ni à la même autorité de surveillance. Il est par exemple admissible, pour une assurance privée, de faire signer à son client une clause de consentement habilitant ladite assurance à collecter ou communiquer des données sensibles. Or, il n'en va pas de même pour l'assurance-maladie obligatoire, dont les traitements de données sensibles sont régis par la législation sur l'assurance-maladie. Un consentement de la personne concernée ne compense en principe pas l'absence de bases légales.

Enfin, il conviendra de développer le recours à des technologies de la vie privée. Ainsi, une pseudonymisation telle qu'initialisée en Allemagne doit être envisagée. En effet, les contrôles effectués par les caisses, notamment l'économicité du traitement, portent avant tout sur les fournisseurs de presta-

tions. Il n'est de ce fait pas nécessaire de travailler avec des données nominatives relatives aux assurés.

Le CAMS ne s'est pas encore prononcé sur notre avis, mais le projet semble suivre son cours, ayant à notre connaissance été présenté à plusieurs reprises dans le cadre de conférences concernant la santé et les assurances.

8.2. Projet de codes à barres sur les factures imprimées

Pour augmenter l'efficacité, il est prévu de munir d'un code à barres les factures imprimées que les médecins envoient à leurs patients afin de permettre aux assureurs de saisir ces factures dans leurs systèmes informatiques à l'aide de ce code à barres.

Fidèle à l'adage « Time is money », on s'efforce, dans le cadre de l'informatisation, de rendre de plus en plus efficaces les procédures de saisie des informations. Une des méthodes utilisées consiste à introduire les informations dans les systèmes informatiques de manière électronique plutôt que de confier cette tâche à un individu. C'est dans cet esprit que les assureurs veulent saisir les factures qu'ils reçoivent des fournisseurs de prestations de manière électronique pour en transférer les données dans leur système informatique. Ce système nécessiterait que les fournisseurs de prestations munissent leurs factures imprimées sur papier d'un code à barres supplémentaire qui fournit toutes les indications nécessaires au remboursement.
On nous a consulté pour savoir si l'utilisation d'un tel code à barres était compatible avec la loi sur la protection des données.
Etant donné que les données personnelles traitées dans les factures des fournisseurs de prestations sont des données sensibles au sens de la loi sur la protection des données, nous somme d'accord avec l'utilisation du code à barres, à condition que :

- seules les données personnelles figurant sur les factures imprimées et traitées de manière licite soient reprises intégralement dans le code à barres ;
- et que le traitement des données personnelles contenues dans le code à barres soit effectué dans le seul but qui est identique à celui qui est à la base du traitement licite des données personnelles figurant sur les factures imprimées.

8.3. Communication par un médecin de données de diagnostic à du personnel soignant de Spitex

Pour permettre le remboursement des frais par les assurances, le médecin doit remplir un formulaire demandant la dispensation de soins par une organisation externe à

l'hôpital (Spitex). Dans ce contexte, la question se pose de savoir si le médecin est autorisé – sur ce formulaire – à communiquer au personnel soignant de Spitex des informations médicales concernant le patient.

Un diagnostic médical mis en relation avec des critères d'identification représente une donnée sensible au sens de la LPD.
Si l'on prend la situation où le médecin prescrivant possède son propre cabinet ou travaille dans un cabinet de groupe organisé selon le droit privé, il doit être considéré comme personne privée au sens de la LPD. Cela signifie donc que la LPD est applicable à la communication de données par ce médecin au personnel soignant de Spitex. Etant donné que Spitex n'est pas une organisation précise, mais un terme utilisé pour regrouper les soins à domicile pouvant être donnés par des personnes et des institutions diverses, il y a lieu pour l'applicabilité de la LPD de distinguer entre le cas où le personnel soignant est organisé selon le droit privé et celui où il intervient en tant qu'employé d'un canton ou d'une commune. Dans les deux derniers cas, la LPD n'est pas applicable au traitement de données personnelles effectué par le personnel soignant. Ce seraient plutôt les dispositions cantonales ou communales en matière de protection des données qui seraient applicables.
Une communication de données n'existe que si les données ont été mises à disposition de tiers. Etant donné que le personnel soignant de Spitex n'est ni subordonné au médecin, ni tenu de suivre les directives de ce dernier, celui-ci doit être considéré comme tiers au sens de la loi sur la protection des données.
Le fait qu'un médecin fournisse des indications concernant le diagnostic médical sur la formule de l'ordonnance doit donc être considéré comme un traitement de données sensibles (communication de données). Le fait que le personnel soignant prenne connaissance du diagnostic médical indiqué sur l'ordonnance constituerait également un traitement de données sensibles (collecte de données).
Une atteinte à la personnalité est contraire à la loi si elle n'est pas justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public ou par la loi. En particulier les données sensibles ne doivent pas être communiquées à des tiers sans motif justificatif.
En principe, le consentement peut être donné soit de manière explicite, soit de manière tacite. L'accord est explicite dans le cas où le patient a par exemple la possibilité d'autoriser, à l'aide d'un formulaire, le médecin à communiquer les données personnelles nécessaires pour les soins au personnel soignant. Un accord tacite par contre existe dans les cas où l'on peut admettre en fonction des circonstances qu'une personne sensée approuve les actes d'une autre personne. Plus les données sont sensibles, plus l'accord devra être clair. C'est pourquoi les exigences envers la qualité des consentements doivent être plus élevées dans les cas où les données à traiter sont des données sensibles (consentement explicite).

Une personne qui accepte des soins à domicile, désire être soignée correctement selon les règles de l'art médical. Cela présuppose que le personnel soignant dispose au moins des informations qui lui sont nécessaires (par ex. présence d'un diabète, d'allergies, etc.) pour dispenser les soins proprement dits. C'est la raison pour laquelle on partira en principe de la possibilité d'un consentement tacite à communiquer les informations indispensables pour les soins au personnel soignant. Un tel consentement tacite ne peut cependant être accepté que pour les informations dont le personnel soignant doit effectivement prendre connaissance dans chacun des cas pour donner les soins. Il y a donc lieu d'examiner chaque cas concret de manière individuelle.
Le consentement tacite comporte le risque d'une incertitude juridique, autant pour le médecin en ce qui concerne son pouvoir à communiquer les données que pour le personnel soignant. Ceci mène à exiger que l'on demande aux patients qui désirent profiter de soins à domicile qu'ils fournissent par écrit un consentement explicite autorisant le médecin à communiquer ces données au personnel soignant. Un tel consentement doit être bien lisible, compréhensible et formulé de manière à ce qu'il informe la personne concernée sur les conséquences de son consentement. Il doit en outre lui donner la possibilité de révoquer ce dernier en tout temps. Conforme au principe de la proportionnalité, ce consentement doit se limiter à la communication des informations dont le personnel soignant a absolument besoin pour donner les soins.
Dans ce contexte, la question se pose également de savoir si le personnel soignant de Spitex est soumis au secret médical.
Selon la loi sur l'assurance-maladie du 18 mars 1994, le fournisseur des prestations doit remettre au débiteur une facture détaillée et compréhensible. Il doit également lui fournir toutes les indications dont il a besoin pour pouvoir vérifier le calcul de la rémunération ainsi que le caractère économique de la prestation. Dans le système du « tiers garant » qui considère que l'assuré est le débiteur, la personne assurée reçoit une copie de la facture, copie qu'elle transmet à l'assureur. L'assureur peut de cas en cas demander un diagnostic précis ou des renseignements supplémentaires d'ordre médical.
Pour le calcul de la rémunération, il peut être utile que l'assureur ait connaissance du diagnostic médical qui a été établi. Le degré de détail du diagnostic doit cependant respecter le principe de la proportionnalité. Cela signifie que seules peuvent être traitées les données qui sont absolument nécessaires pour accomplir la tâche (maxime du minimum absolu). Les informations importantes concernant un patient tel que le diagnostic médical sont transmises à l'assureur par le médecin. A notre avis, le personnel soignant de Spitex n'est en droit de fournir ses prestations que dans le cadre des ordres que le médecin donne pour guérir ce qu'il a diagnostiqué. Il n'est donc pas nécessaire que le personnel soignant fournisse à l'assureur des informations plus détaillées sur le patient. Une telle communication ne serait à notre avis justifiée ni par une norme légale, ni par un intérêt prépondérant privé ou public. Dans la mesure où il n'existe pas de consentement de la personne concernée, ce motif justificatif ne peut donc pas

être avancé. Ceci signifie qu'une communication des données par le personnel soignant à l'assureur constituerait une violation des droits de la personnalité au sens de la loi sur la protection des données.
Une communication de données complémentaires concernant le patient par le personnel soignant tomberait sous le coup de l'article 35 al. 1 LPD. Ce dernier punit quiconque révèle intentionnellement d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité qui ont été portés à sa connaissance dans le cadre de l'exercice de sa profession qui nécessite la connaissance de telles données.

8.4. Taxe à la valeur ajoutée et psychothérapie

Le chiffre d'affaires des psychothérapeutes n'est exclu du champ de la taxe à la valeur ajoutée (TVA) que si une activité reconnue comme traitement curatif est fournie et qu'elle est prescrite par un médecin. Etant donné que les exceptions à l'assujettissement fiscal doivent être prouvées au cas par cas par les contribuables, les personnes traitées doivent consentir à ce que leur nom soit divulgué en relation avec un traitement psychothérapeutique, faute de quoi, le traitement curatif n'est pas exempt de la TVA.

Un psychothérapeute était dérangé de devoir divulguer le nom de ses clients lors de la révision fiscale. Il se demandait en particulier si cette divulgation équivalait à une violation du secret professionnel.
Au terme de notre enquête, il s'avère que les prestations fournies en Suisse sont en principe soumises à la TVA (art. 4 – 6 de l'ordonnance sur la taxe à la valeur ajoutée, OTVA). Ce n'est que pour certaines prestations faisant exception conformément à l'art. 14 OTVA - dont les traitements dans le domaine de la médecine humaine dispensés par des médecins ou des membres d'autres professions apparentées - que le chiffre d'affaires correspondant à ces traitement est exclu ou exempt de la TVA. Les exceptions figurant à l'art. 14 OTVA doivent en outre être interprétées de manière restrictive. Le droit fiscal est soumis au principe généralement reconnu selon lequel les exceptions à l'assujettissement fiscal doivent être prouvées au cas par cas par les contribuables potentiels eux-mêmes. A ce propos, le Tribunal fédéral a établi que même le secret bancaire ne donnait pas le droit absolu de refuser de témoigner ou de fournir des dossiers vis-à-vis des autorités d'enquête. Ainsi, le secret bancaire ne protège pas lorsqu'il s'agit de contrôler si un chiffre d'affaires est soumis ou non à la TVA (ATF 119 IV 175). Par ailleurs, il en va de même des détenteurs de secrets professionnels protégés par la loi. Ainsi, l'avocat qui fait valoir une prestation exempte de la TVA à un client à l'étranger doit donner le nom et l'adresse du client pour que cette prestation ne soit pas soumise à ladite taxe.

Selon le droit en vigueur, les prestations des psychothérapeutes ne sont exemptes de la TVA que si une activité précise, reconnue comme traitement curatif, est fournie et prescrite par un médecin. Pour cette raison, les psychothérapeutes doivent garantir l'accès à leurs dossiers de manière à permettre à l'Administration fédérale des contributions de constater à qui se réfère la prescription du médecin et quelle activité a été fournie en l'espèce. Les données ne peuvent être dévoilées à l'Administration fédérale des contributions que si la personne en traitement a autorisé que son nom soit dévoilé dans le contexte d'un traitement psychothérapeutique (art. 13, 1er al. LPD). Si tel est le cas et s'il s'agit d'un traitement curatif reconnu, la prestation n'est pas soumise à la TVA et sera donc plus avantageuse.
Néanmoins si un client ne veut pas que son nom soit divulgué aux autorités fiscales, le thérapeute ne peut communiquer ce nom aux autorités (violation de l'obligation de garder le secret conformément à l'art. 35 LPD). Dans ce cas, les prestations sont imposables au taux déterminant de 7,5 %.

9. Génétique

9.1. Ordonnance sur l'identification judiciaire à l'aide de profils d'ADN

Suite aux travaux de la commission d'experts « Banque de profils d'ADN » mandatée par le Département fédéral de justice et police, le secrétariat général dudit département a reçu la mission d'élaborer les bases légales nécessaires à une banque de profils d'ADN gérée par la Confédération.

La commission d'experts « Banque de profils d'ADN » mandatée par le Département fédéral de justice et police (voir notre 6ème Rapport d'activités 1998/99, page 285) est arrivé à la conclusion que l'existence au niveau de la Confédération d'une banque de profils d'ADN serait absolument souhaitable et opportune. La mise sur pied ainsi que la gestion d'une telle banque de données nécessite cependant l'existence de bases légales suffisantes. Etant donné qu'une telle banque de profils d'ADN traite des données sensibles au sens de la loi sur la protection des données, ceci nécessite une base légale sous forme d'une loi au sens formel.
Des considérations d'ordre politique avait mené le Département fédéral de justice et police à acquérir la conviction qu'une réglementation par voie d'ordonnance basée sur l'art. 351septies du Code pénal suisse, valable pour une durée limitée jusqu'à la création d'une base légale au sens formel serait suffisante. Le Conseil fédéral a déclaré dans sa réponse à la motion Widmer 99.3068 du 15.3.1999 qu'il allait ordonner l'élaboration d'une telle ordonnance.

En mars 2000, nous avons pris acte de la proposition du Département fédéral de justice et police au Conseil fédéral de mettre en place une banque de profils d'ADN reposant, à titre provisoire, sur une base légale formelle insuffisante au sens de la loi fédérale sur la protection des données. Nous avons déclaré que sans l'approuver, nous ne nous opposions toutefois pas à ce projet pour autant que soit pris l'engagement d'élaborer rapidement la base légale formelle nécessaire.

10. Finances

Banques

10.1. Charges imposées par la Commission de la concurrence dans le cadre d'une fusion

Avant que le nom et l'adresse du client d'une banque soient transmis à d'autres instituts bancaires, les personnes concernées doivent avoir la possibilité de donner leur consentement. La personne désirant demeurer auprès de l'ancienne banque doit le faire savoir. Contrairement aux autres dispositions légales sur la protection des données valables dans d'autres pays, la LPD ne prévoit pas de consentement particulier. Néanmoins, cela ne dispense pas les banques d'informer les clients de manière complète et de leur demander leur avis par écrit.

Des clients de longue date de la banque X nous ont fait part de l'information suivante qui leur avait été transmise par leur banque: selon cette dernière donc, la Commission de la concurrence (Comco) avait décidé que la banque X était tenue de vendre un certain nombre de filiales de son réseau d'agences. Les clients dont il est ici question avaient été choisis au hasard parmi l'ensemble des clients. Ils avaient reçu une lettre dans laquelle il leur était donné la possibilité de changer pour la banque Y. On leur avait également communiqué que leur compte ne serait pas transféré sans leur consentement. Néanmoins, ils étaient tenus de retourner dans un délai de 20 jours le coupon réponse joint dans l'enveloppe prévue à cet effet, sinon la banque X serait tenue de fournir leur nom ainsi que toutes les données nécessaires à l'ouverture d'une relation d'affaires à la banque Y, même sans consentement écrit. Les mêmes informations seraient aussi communiquées si la personne concernée ne retournait pas de réponse écrite d'ici la date limite d'envoi. La banque Y contacterait ensuite les clients pour leur proposer d'établir une nouvelle relation bancaire. Les clients nourrissaient des doutes à propos de cette manière de procéder de la part de la banque et ont voulu savoir si ces doutes étaient fondés.

Après enquête, nous avons constaté que ce procédé était le résultat de l'application de l'accord, approuvé par la Comco en 1998. Selon cet accord, la banque était tenue, si le client ne réagissait pas, de communiquer son nom et ses données personnelles, nécessaires à l'ouverture d'une relation bancaire, notamment en vue de l'adaptation aux produits de la nouvelle banque.
La banque X nous a confirmé que tous les clients concernés avaient été informés par lettre recommandée. Il n'y a pas eu de communication de données pour deux catégories de clients: ceux dont le courrier était déposé dans leur dossier à la banque et qui n'avaient de ce fait rien reçu, ainsi que ceux dont les lettres recommandées n'avaient pas pu être remises ou retirées. La banque X estimait qu'ainsi, chaque client avait eu la possibilité de faire connaître expressément la relation bancaire choisie (consentement explicite). En outre, les clients avaient été informés que s'ils ne retournaient pas le coupon-réponse dans le délai de 20 jours, leurs données seraient transmises à la banque Y. Dans ces circonstances, la banque X estimait qu'il était permis de supposer qu'un client qui ne réagissait pas était tacitement d'accord avec le changement de sa relation bancaire. En d'autres termes, il consentait implicitement à la communication de son nom, de son adresse et des produits bancaires utilisés en vue de l'ouverture d'une relation bancaire avec la nouvelle banque.

Compte tenu de l'ensemble des circonstances, nous sommes parvenus à la conclusion que le procédé choisi concordait avec les dispositions de la législation sur la protection des données.

10.2. Les conditions générales et le consentement donné à des fins de marketing

Les clients doivent être informés du traitement systématique de leurs données à des fins de marketing. Si cette information a lieu par le biais des conditions générales, il faudrait leur donner la possibilité par exemple d'autoriser expressément ou de refuser le traitement de leurs données à des fins de marketing. Le traitement à des fins de marketing ne devrait pas être directement lié à des contrats. En effet, tous les clients ne désirent pas nécessairement de publicité sur les nouveaux produits.

Un client d'une grande banque s'intéressait au telebanking. Mais en lisant les « Dispositions générales relatives à l'utilisation de moyens auxiliaires électroniques » et les « Dispositions spéciales applicables au telebanking et au phonebanking », il nourrit des doutes sur le caractère licite de ces dispositions et nous pria de nous prononcer à ce sujet.
Le passage concernant le traitement des données à des fins de marketing était intéressant du point de vue du droit de la protection des données. Le chiffre 10,

paragraphe 2 des dispositions générales relatives à l'utilisation de moyens auxiliaires électroniques disait : « Par la présente, la banque est expressément autorisée à traiter systématiquement toutes les informations sur ses clients à des fins propres de marketing ». Suite à notre demande de précision auprès de la banque en question, celle-ci a avancé que l'utilisation des données à des fins propres de marketing était expressément mentionnée dans les dispositions générales. Par ailleurs, elle précisa que ce but était non seulement communiqué de manière unilatérale, mais le client donnait son consentement explicite. Nous n'étions pas d'accord sur ce dernier point car un client ne peut consentir explicitement aux conditions générales lorsqu'il n'a pas de possibilité de choix. Dans ces circonstances, le consentement peut à la rigueur être accordé implicitement.

La banque fit valoir en outre que l'on pouvait supposer en toute bonne foi que le produit en question était intéressant pour le client. L'exemple du client qui s'était adressé à nous a montré que cette supposition était fausse. Un client qui s'intéresse au telebanking ou au phonebanking ne souhaite pas automatiquement recevoir de la publicité pour d'autres services.

Nous avons donc signalé à la banque les observations que nous avions déjà faites à ce propos, à savoir que les traitements de données qui ne sont pas en rapport direct avec l'exécution du contrat, par exemple l'utilisation de données à des fins de marketing interne ou externe, ne doivent en aucun cas figurer dans les conditions générales. Imposer à un client un traitement de données qui n'a rien à voir avec l'exécution du contrat ne constitue pas un motif justificatif, ni ne répond au principe de la proportionnalité. Dans ce cas, si le client ne souhaite pas que ses données soient utilisées à des fins de marketing, il est obligé de renoncer aussi à la prestation. Ces traitements de données nécessitent donc une déclaration de consentement séparée de la part du client, déclaration qui ne sera pas liée aux conditions générales. Refuser de livrer ses données personnelles à des fins de marketing ne doit pas avoir de répercussions négatives sur le reste du déroulement du contrat (cf. 5^{e} Rapport d'activités 1997/98, p. 197 s.).
A notre avis, il ne s'agit pas en premier lieu d'une pesée des intérêts entre ceux de la personne concernée et ceux de la banque, car les données personnelles du client ne peuvent être utilisées à des fins de marketing qu'avec le consentement de celui-ci. Pour cette raison, nous avons demandé que le client ait la possibilité de choisir s'il désire ou non consentir à ce que ses données soient traitées à des fins de marketing. Nous avons donc suggéré de modifier ce passage des dispositions générales et d'insérer une clause supplémentaire à la déclaration sur le raccordement au système.
A la suite de cette recommandation, la banque a mandaté une expertise et nous a communiqué qu'elle estimait non contraignant du point de vue juridique l'octroi d'une possibilité de libre choix conçue comme élément séparé du contrat. Elle se déclara néanmoins prête à préciser la clause dite de marketing. Désormais,

cette clause doit indiquer clairement que toutes les données potentielles de marketing sur un client ne seront pas traitées à des fins de marketing, mais seulement celles qui découlent de la relation bancaire. En outre, la clause de marketing sera désormais imprimée en caractère gras.
Les personnes concernées peuvent néanmoins refuser en tout temps le traitement de leurs données à des fins de marketing, sans que cette décision implique des conséquences négatives.

10.3. Identification des clients de la banque au guichet

La personne qui désire entamer de nouvelles relations commerciales avec une banque doit fournir la preuve de son identité. Pour sa part, la banque est tenue, pour des raisons de preuve et de sécurité, d'identifier les nouveaux clients et d'établir leur identité de manière adéquate. Ces prescriptions d'identification ont heurtées tout particulièrement les clients de longue date, lesquels se sont adressés à nous pour s'informer des conditions de l'identification et du traitement de leurs données personnelles au guichet de la banque.

Nous recevons régulièrement des demandes de personnes qui sont priées de présenter au guichet de leur banque une pièce d'identité, laquelle est ensuite photocopiée. Bon nombre d'entre elles s'insurgent contre cette procédure qui ne leur semble pas suffisamment justifiée. Conformément à l'art. 2 de la Convention relative à l'obligation de diligence des banques (CDB 98) de l'Association suisse des banquiers (ASB), les banques sont tenues d'identifier le partenaire contractuel lors de l'ouverture de relations commerciales. Cette règle est notamment applicable à l'ouverture de comptes, de livrets ou de dépôts, à l'exécution d'affaires fiduciaires, à la location de coffres, à l'acceptation de mandats de gestion de fortune auprès de tiers ou encore aux opérations au comptant portant sur des sommes supérieures à Fr. 25 000.

Conformément aux prescriptions générales en matière d'identification, il convient d'établir de manière appropriée le nom, le prénom, la date de naissance, la nationalité et l'adresse du domicile du client, ainsi que les moyens avec lesquels l'identité a été contrôlée. La banque doit conserver la photocopie de la pièce officielle d'identité ainsi que les autres documents ayant permis l'identification pour que la révision interne et le service de révision prévu par la loi sur les banques puissent contrôler l'accomplissement de l'identification (Art. 2 N 20 + 21, Prescriptions générales d'identification et surveillance, CDB 98).

Dans la pratique, les circonstances régies par l'art. 2 CDB sont courantes, mais les employés de la banque devraient les expliquer au client. Par exemple, l'ouverture d'un dépôt est absolument nécessaire lors de l'achat d'obligations. Donc, il est impossible d'acheter des obligations sans photocopie des papiers d'identité.

Suite à la révision de la CDB du 1er juillet 1998, les clients de longue date ont dû également fournir à leur banque une copie de leur pièce d'identité, leur date de naissance ainsi qu'une photo, ce qui a suscité une incompréhension massive de la part de plusieurs clients. Dans de nombreux cas, cette demande avait été faite sans que le client en soit suffisamment informé. Nous avons donc suggéré à ces personnes de s'adresser directement à la banque afin d'obtenir, selon les faits, la raison effective de cette copie. Par ailleurs, du fait que ce genre de traitement de données personnelles n'est pas en premier lieu un cas régi par la loi sur la protection des données, mais concerne les règles internes d'organisation bancaires, il est possible de s'adresser au médiateur des banques suisses.

10.4. Entraide administrative entre la Commission fédérale des banques et la « Securities and Exchange Commission » des Etats-Unis d'Amérique

La transmission de données personnelles par la Commission fédérale des banques à la «Securities and Exchange Commission» constitue à notre avis un cas d'entraide administrative, laquelle est prévue par la LPD. Mais parallèlement à la LPD, les dispositions spécifiques de la loi fédérale sur les bourses relatives à l'entraide administrative sont ici également applicables.

Un avocat nous a signalé que la Commission fédérale des banques (CFB) avait l'intention de communiquer des données personnelles de clients d'une banque suisse à la « Securities and Exchange Commission » (SEC). La SEC reconnaîtrait ouvertement vouloir publier toutes les procédures pour délit financier présumé en mentionnant sur son site Internet le nom et le comportement des personnes concernées, cela avant qu'un tribunal indépendant ait statué sur les cas en question. La plupart des comportements reprochés à ces personnes constitueraient en Suisse un état de fait constitutif de l'infraction, qui n'aurait néanmoins pas fait l'objet d'une constatation judiciaire. De ce fait, la publication sur Internet violerait le principe de la présomption d'innocence en vertu de l'art. 6, chiffre 2 de la Convention européenne des droits de l'homme. Par ailleurs, les données seraient ainsi accessibles à l'ensemble des autorités étatiques en violation du principe de spécialité et être alors utilisées dans le cadre de

procédures administratives, fiscales ou pénales sans qu'il y ait de réserves relevant de l'Etat de droit. Le traitement des données personnelles effectué par la SEC violerait de ce fait gravement la personnalité des personnes concernées. La LPD interdit la communication de données personnelles à l'étranger lorsque celle-ci risque de menacer gravement la personnalité des personnes concernées.
De l'avis de la CFB, que nous avons contactée, la LPD n'est pas applicable à l'entraide administrative (application par analogie de l'art. 2, 2e al. lettre c LPD concernant l'entraide judiciaire). La CFB fonde son argumentation sur le fait que dans le cas précis, il s'agirait d'une procédure d'entraide judiciaire internationale, donc que la LPD n'était pas applicable. Elle estime en outre que l'art. 38 de la loi sur les bourses, en tant que loi spéciale, prime les dispositions générales de l'art. 6 LPD. Nous ne pouvons partager ce point de vue. La doctrine traite l'entraide administrative et l'entraide judiciaire de manière séparée. Les délits relevant de l'entraide judiciaire, passibles d'une sanction pénale, présentent des structures complexes à propos de l'établissement des faits en relation avec l'étranger. En général, l'établissement des faits dans les affaires pénales requiert le recours à la procédure d'entraide judiciaire internationale qui prévoit que les requêtes doivent être adressées à l'Office fédéral de la police (OFP). La procédure de l'entraide administrative internationale est en revanche informelle si les informations échangées ne se réfèrent pas à des personnes. L'argumentation selon laquelle la LPD ne serait pas applicable à l'entraide administrative internationale par analogie à l'entraide judiciaire n'est pas défendable dans ce contexte. Il ne ressort pas de la LPD qu'elle ne serait pas applicable à l'entraide administrative internationale. La LPD renferme même des normes en matière d'entraide administrative dans le contexte intérieur suisse et dans le contexte international.
Nous estimons qu'il est erroné de prétendre que l'art. 38 de la loi sur les bourses (LBVM), du fait de sa spécialité, prime la LPD et, de ce fait, l'art. 6 LPD. La LPD est applicable au traitement de données par les organes fédéraux tels la CFB. Le droit fédéral ne contient pas de normes générales sur l'entraide administrative. Néanmoins, certaines dispositions spécifiques sont applicables et, pour ce qui est des données personnelles, il convient de se référer aux articles 19 et 20 LPD dont on peut déduire des critères généraux qui sont applicables d'une manière générale à l'entraide administrative (cf. également la pratique constante de la CFPD in JAC 1998 II 39 et 40).
La transmission de noms par la CFB à la SEC à des fins de publication sur Internet – en dehors d'une procédure pénale – n'est pas en accord avec la disposition spéciale sur l'entraide administrative internationale de l'art. 38, 2e al. LBVM. En effet, les conditions pour la communication d'informations non accessibles au public et de documents y relatifs à des autorités étrangères de surveillance des bourses et des courtiers en bourse ne sont pas remplies. Pour que la protection de la personnalité soit garantie, il faut donc que les principes généraux de la protection des données, y compris l'art. 6 LPD sur la communication de données personnelles à l'étranger, soient applicables. La

communication de données personnelles par la CFB à la SEC n'est donc pas justifiée.

Le litige est actuellement en suspens auprès du Tribunal fédéral.

Sociétés de renseignements économiques

10.5. Comparaison des données lors d'un examen de solvabilité

Dans le domaine de la grande distribution, il n'est pas toujours possible de vérifier la solvabilité de tous les clients potentiels. Dans la mesure où les sociétés de renseignements économiques cryptent les données personnelles avant de les communiquer à ses clients (vendeurs) et que ceux-ci ne reçoivent, après comparaison des données, que celles dont ils ont besoin pour la conclusion ou l'exécution d'un contrat, il s'agit d'une comparaison de données conforme à la législation sur la protection des données.

La recommandation du 18 décembre 1998 concernant la comparaison des données lors d'un examen de solvabilité (cf. 6ème Rapport d'activités 1998/99, p. 184), a été acceptée par le maître du fichier. Il était prêt à examiner un nouveau produit ne fournissant plus à ses clients (vendeurs) que des données sous forme cryptée. Avec ce nouveau fichier, la comparaison automatique des données (matching) continuera à être effectuée, mais dans le cadre d'une procédure dite de la boite noire, au cours de laquelle les données de l'acheteur sont codées avant d'être automatiquement comparées avec les données sur la solvabilité des personnes à risque. Après la comparaison, le vendeur ne reçoit plus que les données dont il a besoin pour la conclusion ou l'exécution d'un contrat. Cette méthode empêche l'accès non autorisé à des données sur la solvabilité d'autres personnes ou la copie des supports de données dans le but d'utiliser les données à d'autres fins.

Les vendeurs doivent s'identifier à l'aide d'un numéro d'identification d'utilisateur et d'un mot de passe personnel. En outre, à chaque consultation, l'utilisateur doit confirmer en appuyant sur une touche que la consultation a lieu en vue de la conclusion d'un contrat (commande de marchandises ou de services) ou en relation avec l'exécution d'un contrat, par exemple pour enquêter sur une créance non recouvrée en vue de l'introduction d'une poursuite. Les consultations opérées par les utilisateurs font l'objet d'une journalisation pour des raisons de sécurité et d'établissement des preuves.

Le respect des prescriptions de protection des données ont été réglées par contrat, le maître du fichier ayant le droit de contrôler le respect des charges.

10.6. Rappels de paiement et données erronées conservées par des sociétés de renseignements économiques

Au cours de l'année écoulée, les données erronées ou complètement obsolètes se sont accumulées dans divers fichiers de sociétés de renseignements économiques. Nous avons donc souligné à plusieurs reprises le fait qu'il fallait vérifier régulièrement l'exactitude et l'actualité des données et effacer les données obsolètes. Les données fausses constituent un préjudice non seulement pour les personnes concernées, mais aussi pour les acheteurs de ces données. Lorsque des données relatives à des rappels de paiement sont communiquées, il est contesté que ces données soient appropriées et utiles à l'appréciation de la solvabilité.

Diverses sociétés de renseignements économiques ont indiqué à leurs clients des rappels de paiement en guise d'informations sur la solvabilité de certaines personnes, avant ou parallèlement à l'ouverture d'une poursuite. Nous estimons que les rappels de paiement ne permettent pas de tirer des conclusions utiles sur la solvabilité d'un client potentiel. En cas de créances controversées, il est possible que des rappels de paiement soient envoyés, mais il est disproportionné de les communiquer à des tiers avant que la justesse de la créance soit vérifiée. Depuis des années, nous demandons à toutes les sociétés de renseignements économiques que les données ne soient transmises à des tiers qu'après introduction de la demande d'ouverture de la poursuite. Nous avons donc à plusieurs reprises attiré l'attention des maîtres de fichiers à ce propos. Depuis, une entreprise a effacé toutes ses données relatives aux rappels de paiement. D'autres continuent à fournir les données après ouverture de la poursuite, ce qui n'est pas en accord avec les principes généraux de la protection des données.

Le cas présenté ci-dessous est représentatif de divers exemples de traitement de données obsolètes en relation avec la capacité de payer. En 1994, une personne soigna durant quelque temps ses parents très malades, qui décédèrent rapidement. Accablée de travail, cette personne oublia, durant toute la période qu'elle consacra à ses parents, de régler à temps quatre factures, dont les montants allaient de Fr. 140.- à Fr. 560.- et fut poursuivie à bon droit. Toutefois, après la mort de ses parents, elle régla l'ensemble des créances, y compris les intérêts moratoires. Personne ne demeura donc lésé. Lorsqu'en 1999, elle désira signer un contrat de vente, il lui fut répondu qu'elle n'était pas solvable. Selon le résultat des recherches effectuées ultérieurement, ses données personnelles, vieilles de plus de cinq ans, étaient encore en circulation ou avaient été vendues, raison pour laquelle elle avait été considérée comme non solvable. Suite à notre intervention, les données en question ont été effacées par la société de renseignements économiques.

11. Publicité et marketing

11.1. Nouvelles méthodes pour l'étude de marché: saisie informatique des achats des consommateurs

Le secteur du marketing est en constante évolution. Tout nouveau développement qui apparaît sur le marché est immédiatement évalué quant à son potentiel d'utilisation pour l'optimisation des bénéfices. Dans le domaine des études de marché par exemple, on constate une évolution de l'utilisation de questionnaires conventionnels vers des méthodes de relevé techniques. Il semble que l'imagination dans ce domaine ne connaisse pas de limites.

Par l'intermédiaire des médias ainsi que suite à des indices fournis par la population, nous avons été rendu attentif à une nouvelle méthode d'étude de marché qui représente un fait tout nouveau pour nombre de consommateurs. Contrairement à la méthode bien connue de sondage à l'aide de questionnaires, on utilise des scanners – de manière analogue aux systèmes de fidélisation tels que le système M-Cumulus – qui permettent aux participants au projet (consommateurs) de saisir eux-mêmes leurs achats pour ensuite transmettre les données concernant leurs achats par ligne téléphonique au serveur de l'entreprise qui effectue l'étude de marché. Le but de ce nouveau système d'enregistrement des produits est d'optimiser les résultats des études de marché traditionnelles concernant le comportement du consommateur. Les questionnaires servent dès lors uniquement à classer les consommateurs dans des catégories prédéfinies (selon l'âge, le sexe, la profession, la région, etc.) alors que la saisie avec le scanner permet d'enregistrer le comportement effectif du consommateur.
Les statistiques sur le comportement des consommateurs servent à vendre aux clients du bureau d'études de marché (producteurs et revendeurs de biens de consommation) des informations sur le comportement des consommateurs afin que ceux-ci puissent développer et améliorer leurs stratégies commerciales.
Comme nous l'avons déjà relevé dans nos articles précédents sur le thème des études de marché (voir le 5ème Rapport d'activités 1997/98, pages 210 ss et le 6ème Rapport d'activités 1998/99, pages 298 ss), nous considérons qu'une information suffisante des personnes participant au test sur les traitements de données prévus est absolument nécessaire. Les personnes concernées doivent absolument savoir quelles sont les données qui sont enregistrées et comment celles-ci sont traitées de cas en cas. Il est particulièrement important de communiquer préalablement aux participants au test quelles sont les données les concernant qui sont traitées (par ex. quelle information est munie d'un code à barres), comment et dans quel but ces données sont traitées (par ex. la transmis-

sion de données personnelles à des tiers) et pour quelle durée ces données sont conservées.

Les personnes concernées ne peuvent donner leur consentement pour un traitement de données de manière légalement valable que si elles connaissent l'envergure exacte des traitements de données qui sont prévus. Le but du traitement doit déjà ressortir de la lettre d'accompagnement ainsi que d'une clause de consentement qui doit être formulée de manière précise et apposée à un endroit bien visible du formulaire de demande. La transparence lors du traitement de données personnelles est une exigence fondamentale de la protection des données et représente en outre une condition essentielle, apte à inciter la confiance, dans les relations d'affaires.
En ce qui concerne la portée du droit d'accès, nous tenons une nouvelle fois à relever ici que l'entreprise qui fait l'étude de marché doit communiquer à la personne requérante toutes les données qu'elle traite sur le compte de cette dernière. Ceci n'englobe pas seulement les données relatives à la consommation ainsi que les analyses de marché (appartenance à une certaine catégorie de consommateurs) qui ont été établies à ce propos, mais également les critères selon lesquelles les personnes de test potentielles ont été sélectionnées ainsi que les données qui ont été mises à disposition de l'entreprise d'études de marché concernée par le biais d'autres moyens (par exemple en remplissant le formulaire de demande).

11.2. Aide-mémoire "SPAM: Qu'est-ce et comment s'en protéger"

Cet aide-mémoire donne un aperçu des possibilités techniques et juridiques pour se protéger de la publicité non désirée effectuée par e-mail. Voir annexe page 238.

12. Statistiques

12.1. Protection des données et utilisation des données à des fins statistiques : perspectives d'avenir

Les données personnelles peuvent être utilisées presque sans restriction à des fins statistiques. La loi sur la protection des données (LPD) et la loi sur la statistique fédérale (LSF) prévoient en effet des conditions plus souples dans ce but. Néanmoins, tout traitement de données, dans le domaine de la statistique comme de la protection des données, est soumis à une condition fondamentale : le principe de finalité.

Selon le principe de finalité, les données personnelles relevées à des fins statistiques ne peuvent être utilisées à d'autres fins (par exemple des fins administratives). L'art. 14 LSF prévoit néanmoins une exception à ce principe lorsqu'une loi fédérale l'autorise expressément ou que la personne concernée y a consenti par écrit.
Nous estimons qu'à l'avenir, l'établissement de recueils ou de fichiers centraux doit être fait avec retenue. En effet lorsque ces fichiers sont opérationnels et utilisés comme instruments de rationalisation, il devient très vite tentant d'utiliser cette rationalisation comme argument pour passer outre le principe de finalité établi par la LPD et la LSF, ou bien d'utiliser les données à d'autres fins (administratives ou économiques). Ce n'est un secret pour personne, l'utilisation de fichiers statistiques permet de faire des économies dans d'autres domaines. La pression exercée sur des banques de données considérées comme anodines en vue d'une utilisation élargie de ces données s'accroîtra donc.

Les travaux statistiques impliquant des données personnelles devront à l'avenir satisfaire aux conditions suivants :

- Utiliser plus souvent les fichiers existants pour établir les relevés statistiques et collecter moins de données directement auprès des personnes concernées.
- Utiliser des procédés techniques de sécurité qui garantissent les droits de la personnalité des personnes concernées et la sécurité des données (notamment procédés de transmission sûrs et méthodes de cryptage).
- Mettre en place des mécanismes permettant l'utilisation de pseudonymes; ils limitent le traitement de données personnelles et sont ainsi plus respectueux du principe de finalité sans pour autant diminuer la qualité des travaux statistiques.

- Recensement de la population 2000 – un recensement de transition

Le prochain recensement de la population sera transitoire dans la mesure où il permettra de passer du relevé général par formulaire aux recensements fondés sur les registres. Les registres actuels seront donc restructurés de manière à être utilisés dorénavant de manière optimale à des fins statistiques. Il s'agit néanmoins d'une exception unique au principe de finalité. Ultérieurement, les données personnelles relevées dans le cadre du recensement de la population ne devront plus servir à mettre à jour les registres administratifs.

- Registre des bâtiments et logements

Le registre des bâtiments et logements sera également constitué à partir de données du recensement. Ce projet audacieux a pour but d'utiliser à l'avenir les données des registres à des fins statistiques. Toutefois, il n'y aura pas d'apport constant de données statistiques dans le registre des bâtiments et logements. Seules les données statistiques tirées du recensement 2000 pourront être utilisées afin de mettre sur pied ce registre, qui sera également utilisé à des fins administratives. Tout comme pour le prochain recensement, il s'agit ici d'une exception unique.

L'Office fédéral de la statistique pourra utiliser ce registre national à des fins statistiques et les cantons aussi à des fins administratives. Néanmoins, ces derniers ne pourront utiliser que les données concernant leur territoire. Parallèlement, les cantons seront chargés de mettre à jour les données figurant dans le registre des bâtiments et logements.

II. AUTRES THÈMES

1. Datawarehousing et datamining

1.1. Datawarehousing, datamining et principe de finalité

Le datawarehousing et le datamining impliquent une modification fondamentale du déroulement usuel des traitements de données. Il s'agit de procédés électroniques qui permettent d'obtenir, à partir de données personnelles, des résultats instructifs sur le comportement des individus. Les informations potentiellement utiles sont systématiquement exploitées. Ces technologies sont susceptibles de violer les dispositions du droit de

la protection des données. En effet, le principe de finalité pose des limites au traitement de données personnelles effectués à l'aide de ces technologies.

Le datawarehousing et le datamining permettent aux entreprises d'exploiter de grandes quantités de données. Leur but est d'obtenir, par le biais de traitements et d'analyses, un certain nombre d'informations sur le comportement de leurs clients à partir de données internes. Elles obtiennent ainsi, sur ces personnes, de nouvelles informations qui n'ont plus rien à voir avec le but initial indiqué et peuvent les utiliser en outre pour anticiper le comportement des clients. Dans un cas extrême, un client pourrait faire l'objet d'une mesure spécialement mise au point pour lui. Les données ne sont alors plus exclusivement en relation avec le but pour lequel elles ont été à l'origine relevées, mais elles servent aussi tous les autres buts d'utilisation qui existent ou pourraient éventuellement exister.

Ces informations supplémentaires dont la finalité n'est définie que lors de l'exploitation sont incompatibles avec le principe de finalité. Dans ce genre de cas, même un consentement de la personne concernée lors du relevé des données n'apporte rien car le but de l'utilisation ne peut lui être donné avec précision. La personne concernée n'est plus en mesure de contrôler les traitements de données sur sa personne parce qu'elle ne peut pas savoir comment ses données personnelles seront exploitées.

L'application actuelle de ces méthodes de traitement de données ne sont pas compatibles avec les principes généraux de protection des données (voir également à ce sujet le 6ème Rapport d'activités 1998/99, p. 304 s.).
Nous recommandons donc aux entreprises qui désirent utiliser les procédés de datawarehousing ou de datamining, ou d'autres procédés similaires, d'examiner la compatibilité du traitement des données envisagé avec le principe de finalité. Ces entreprises devraient en outre s'assurer que les personnes concernées sont clairement informées du sort réservé à leurs données et puissent exercer un contrôle. Dans ce cas, le traitement électronique de données personnelles ne pourrait produire que des informations dont les personnes concernées ont été avisées ou qui sont couvertes par le but du relevé.

2. Carte-client

2.1. Remise d'adresses de clients au juge d'instruction

Lorsqu'un personne jette son ticket de caisse avec numéro M-Cumulus dans un sac poubelle qui n'est pas déposé correctement, elle doit s'attendre à ce que les autorités d'investigation parviennent à obtenir son adresse. En demandant une carte M-Cumulus,

le client de la Migros n'autorise en principe que le traitement de ses données par ladite entreprise. Pourtant, un juge d'instruction peut se fonder sur la loi pour demander à la Migros de lui communiquer le nom et l'adresse de la personne contre qui une plainte a été déposée.

Le titulaire d'une carte M-Cumulus avait jeté un ticket de caisse (sur lequel figure le numéro de carte Cumulus) dans sa poubelle à la maison. Il avait ensuite déposé le sac poubelle sans vignette, à la lisière d'une forêt. Dans le but de trouver l'auteur de l'infraction, le juge d'instruction s'adressa à la Migros qui est maître du fichier et la pria de lui communiquer le nom et l'adresse de l'auteur présumé. La Migros ne savait pas si elle était ou non autorisée à communiquer ces données personnelles au juge d'instruction. En effet, dans le formulaire de demande de sa carte-client, elle s'engage à ne traiter les données qu'au sein de la coopérative Migros à des fins de statistiques ou de marketing et à ne pas les transmettre à des tiers extérieurs.

Les circonstances dans lesquelles il est justifié de communiquer des données personnelles à un juge d'instruction doivent être examinées sous l'angle du droit de refuser de témoigner. En principe, seuls les ecclésiastiques, avocats, défenseurs en justice, notaires, contrôleurs et professionnels de la médecine ainsi que leurs auxiliaires ont le droit de refuser de témoigner (Art. 321 Code pénal, CP). Toutes les autres personnes soumises au secret professionnel ou contractuel sont en général tenues de témoigner en procédure pénale dans la mesure où un code de procédure pénale ne connaît aucune autre exception. Le code de procédure pénale du canton en question prévoit que les personnes citées à l'art. 321 CP ne peuvent être obligées de témoigner. En outre, les fonctionnaires pourraient refuser de témoigner eu égard au secret de fonction dans la mesure où les autorités supérieures n'ont pas approuvé l'audition. Par contre, les personnes privées comme la Migros ne sont pas nommées. Etant donné cette base légale, nous avons conclu qu'il était justifié de communiquer au juge d'instruction le nom et l'adresse du titulaire d'une carte-client, déterminés à partir du numéro de carte.

3. Clauses de consentement

3.1. Conditions que doivent remplir les déclarations de consentement

Un traitement de données n'est pas contraire au droit notamment si la personne concernée a donné son consentement. Celui-ci doit répondre à certaines conditions. Or la

pratique montre que bon nombre de déclarations de consentement présentent des lacunes.

Tout un chacun possède le pouvoir de décision sur ses données personnelles ; il s'agit du droit à l'autodétermination individuelle en matière d'information, qui a pour but de permettre à la personne concernée de garder une vue d'ensemble du ou des traitements auxquels ses données sont soumises. Il en va de même lorsqu'elle donne son consentement au traitement de ses données.
Un traitement de données n'est pas illicite lorsqu'un motif le justifie. Le consentement de la personne concernée fait partie des motifs justificatifs. Il occupe d'ailleurs actuellement une place de plus en plus importante, surtout dans le secteur privé.
Selon la définition, le consentement est une déclaration de volonté qui a lieu sans contrainte pour un cas concret et en toute connaissance de cause, et par lequel la personne concernée accepte que des données le concernant personnellement soient traitées.
Le consentement peut avoir lieu de manière *explicite*. Dans ce cas, il n'est lié à aucune forme et peut donc avoir lieu oralement ou par écrit. Il peut aussi *découler de l'ensemble des circonstances*, donc être tacite. Néanmoins, l'absence de déclaration ne veut pas dire qu'il y a consentement tacite. Par ailleurs, le consentement peut être *présumé*, par exemple dans une situation d'incapacité momentané de jugement.
Forte du droit à l'autodétermination individuelle en matière d'information, la personne concernée donne son consentement *de son plein gré*. La question de savoir si et dans quelle mesure le plein gré est applicable dans la pratique demeure en suspens. La pratique montre néanmoins que partout où règnent des rapports de force économique, un consentement de plein gré est illusoire. Par exemple, il est douteux que les analyses d'urine effectuées dans le cadre du recrutement d'apprentis puissent être volontaires (cf. 6ème Rapport d'activités 1998/99, p. 257 à 259). Même si le plein gré de ces tests est souligné, le futur apprenti acceptera en général de s'y soumettre par crainte de ne pas être choisi. En effet, les places de stage ne sont pas si faciles à trouver de nos jours.
Par ailleurs, un consentement est révocable en tout temps. Cette révocabilité est la conséquence du droit à l'autodétermination individuelle en matière d'information, applicable en tant que droit absolu en tout temps et à l'égard de tous.
Les principes posés par la législation sur la protection des données sont également essentiels. Selon le principe de finalité, les données ne peuvent être traitées que dans le but initialement prévu. Un consentement peut néanmoins mener à une modification de la finalité. Par exemple, si une compagnie d'assurance désire traiter les données de ses clients à d'autres fins, comme le «cross-selling», elle doit auparavant recueillir le consentement des personnes concernées.

Toutefois, pour qu'un consentement soit valable, il est déterminant que la personne concernée perçoive la portée (surtout l'ampleur et le but) de ce consentement. Plus les données sont sensibles, plus le consentement doit répondre à des critères de transparence élevés. C'est effectivement le manque de transparence des déclarations de consentement qui constitue le nœud du problème dans la pratique.
Couramment utilisées, les «procurations générales» ont un contenu très global et ne permettent pas d'apprécier l'ampleur du traitement de données envisagé. Ce sont en fait des clauses de consentement si standardisées qu'elles risquent de transformer le consentement en simple formalité. En particulier, ces procurations ne suffisent pas à délier le médecin du secret médical, comme cela se pratique couramment dans les assurances. Le consentement doit toujours être donné au cas par cas (cf. également 6ème Rapport d'activités 1998/99, p. 272/273).
Lorsqu'une entreprise traite des données personnelles à l'aide de techniques modernes telles le datawarehousing ou le datamining, il est permis de douter que les personnes concernées aient vraiment donné leur consentement. En effet, ce genre de méthodes ne permettent fondamentalement pas de prévoir le but du traitement de données effectué (cf. 6ème Rapport d'activités 1998/99, p. 304/305, ainsi que p. 193 du présent rapport).
Enfin, la portée du consentement ne doit pas restreindre excessivement la liberté des personnes concernées. En d'autres termes, le traitement de données doit être approprié et nécessaire au but poursuivi (principe de la proportionnalité). Par exemple, un consentement qui habiliterait un médecin à répondre à toute question sur l'état de santé de la personne concernée irait trop loin. Il serait également disproportionné qu'un médecin puisse donner des renseignements à ce propos sans limite dans le futur.

4. Protection des données et entreprises de transport

4.1. Le projet «EasyRide» des entreprises de transport public

Sous le nom «EasyRide», les entreprises de transport public prévoient d'introduire en Suisse le titre de transport électronique. Ce système devrait permettre à chacun de voyager de manière commode en utilisant sa carte à puce et de ne payer ses trajets qu'après coup. Ce système entraîne des traitements importants de données personnelles. Nous avions déjà été contacté au début de 1998 au sujet de ce projet et avons eu à plusieurs reprises la possibilité de nous informer et de donner notre avis sur les dispositions applicables en matière de protection des données.

Ces derniers temps de plus en plus d'activités de la vie quotidienne laissent des traces (caméras vidéo, retrait d'argent au terminal bancaire, achat avec une carte client, télécommunications, etc.). Ceci a pour conséquence que la sphère dans laquelle il est possible d'évoluer de manière libre sans être observé, devient de plus en plus restreinte. Dans l'optique de la protection de la personnalité, il faut donc autant que possible éviter de créer de nouveaux fichiers et de procéder à des dépouillements de ceux-ci. Au vu des risques pour la sphère privée, il y a lieu de peser les intérêts des maîtres de fichiers et les risques potentiels d'atteinte à la personnalité.

La liberté de mouvement expressément garantie par la Constitution comme faisant partie de notre liberté personnelle garantit non seulement notre droit de nous mouvoir en toute liberté, mais également celui de ne pas être systématiquement observé lors de ces mouvements. Un enregistrement permanent et complet de nos mouvements peut perturber ou restreindre ces derniers.

Dans le cadre du projet «EasyRide» des entreprises de transport public suisses, il est prévu de traiter des données personnelles détaillées relatives à l'utilisation (jusqu'ici anonyme) des transports publics. Il s'agit entre autres des lieux et des heures où le voyageur est monté à bord, puis descendu du moyen de transport ainsi que des données nécessaires à la facturation. Ces données permettent de constituer des profils précis des déplacements de personnes puisque l'on sait exactement qui a pris quel moyen de transport où et quand pour se rendre où et combien ce trajet lui a coûté. Même lors d'une utilisation peu importante des transports publics, ces données peuvent constituer des profils de la personnalité. Les profils de la personnalité sont spécialement protégés par la loi sur la protection des données. Leur traitement n'est possible que dans certaines conditions.

Il est en outre possible d'analyser l'usage que des millions de clients font des transports publics à l'aide d'autres techniques (le datamining par ex.) et de mettre ces données en relation avec d'autres pour en tirer de nouvelles informations. De tels traitements sont souvent difficilement décelables par les personnes concernées. Même si celles-ci en sont informées, elles peuvent rarement se faire un idée de l'envergure des traitements de données qui sont possibles.

Sur la base des principes énoncés dans la loi sur la protection des données, nous pouvons déduire les exigences suivantes envers «EasyRide»:

- Le nouveau système «EasyRide» doit continuer à offrir au client une possibilité d'utiliser les moyens de transport en restant anonyme, à savoir que cette possibilité doit garantir qu'aucune donnée personnelle et encore moins un

profil de la personnalité puisse être créé concernant l'utilisation qu'il fait des transports publics.

- Le fait de choisir le mode d'utilisation anonyme ne doit en aucune manière discriminer le client, notamment au niveau du prix.

- Les clients qui ont pris la décision d'utiliser le mode non anonyme doivent être préalablement informés en détail et de manière compréhensible sur tous les traitements de données personnelles (en particulier la communication éventuelle de données à des tiers) et sur le but de ces derniers.
- Les données personnelles ne doivent être conservées que pour la durée nécessaire pour atteindre les buts prévus et acceptés par le client. Les données doivent ensuite être anonymisées ou détruites.

- Les mesures organisationnelles et techniques adéquates doivent être prises pour éviter tout traitement illicite des données personnelles.

Dans sa réponse de mars 1999 à la question ordinaire du conseiller national Hans Widmer (98.1185), même le Conseil fédéral a en outre souligné qu'il était important de respecter la protection des données dans le projet «EasyRide».

Sur la base des informations que nous possédons et des entretiens que nous avons eu avec les responsables de ce projet, nous avons constaté que ces derniers ont la volonté de respecter les exigences de la protection des données. Il est cependant nécessaire que nous continuions à accompagner ce projet afin d'être en mesure d'apprécier les questions de protection des données qui apparaîtront au cours de sa concrétisation.

5. Publication de données personnelles

5.1. La publication de polices d'assurance « en déshérence »

L'Etat de Californie demande aux compagnies d'assurance le nom des titulaires des polices d'assurance « en déshérence » contemporaines de l'holocauste. Ces données devraient être accessibles au public. Or, le droit de la protection des données n'autorise cet accès que dans certaines conditions.

La Californie projette d'établir un registre répertoriant le nom des titulaires de polices d'assurance conclues entre 1920 et 1945. Cet Etat fédéral américain a

donc mis en demeure les assurances de lui fournir les données sur leur clientèle couvrant cette époque. Des amendes et le retrait de la licence d'assurance menaceraient les compagnies qui n'obtempéreraient pas. Ces données devraient par ailleurs permettre d'établir une banque de données accessible au public. La loi en question (Knox Bill) est entrée en vigueur le 8 octobre 1999. Une compagnie d'assurance suisse nous a demandé si la communication de ces données aux Etats-Unis était admissible.

Les données personnelles ne peuvent être communiquées à l'étranger que si la personnalité des personnes concernées ne s'en trouve pas gravement menacée. L'absence d'une protection des données comparable à celle dont nous disposons en Suisse est considérée comme une violation de la personnalité. Le PFPD possède une liste des Etats disposant d'une législation sur la protection des données comparable à celle de la Suisse. Il est incontestable, dans ce contexte, que les Etats-Unis ne disposent pas d'une protection des données de niveau comparable. Il est donc permis d'admettre qu'il y a violation grave de la personnalité lorsque des données personnelles sont transmises de Suisse en Californie.

Néanmoins, lorsque le droit étranger n'offre pas de garanties suffisantes en matière de protection des données, il est possible de prendre les mesures de protection nécessaires par voie contractuelle. Les contrats ont pour but de garantir les droits de la personnalité de la personne concernée à l'étranger aussi. Le Conseil de l'Europe a élaboré à cet effet un contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données (cf. également 3ème Rapport d'activités 1995/96, p. 207 à 210 et 250 à 253). Mentionnons encore à ce propos que les fichiers qui sont transmis à l'étranger doivent être annoncés auprès du PFPD.

Le PFPD n'est pas en mesure de juger si la Knox Bill assurera une protection moindre que la loi suisse sur la protection des données. Mais, avant que la Californie puisse constituer une banque de données où les données personnelles seront accessibles au public, ainsi qu'il est manifestement prévu, il convient de prendre toutes les mesures restreignant l'atteinte aux droits de la personnalité des ayants droit (principe de la proportionnalité). En particulier, il convient d'entreprendre auparavant tous les efforts possibles pour que les ayants droit puissent être contactés directement. C'est également ce que nous avions fait auprès des banques à propos des fonds en déshérence (cf. 5ème Rapport d'activités 1997/98, p. 212/213).

Néanmoins, si les Etats-Unis ne peuvent garantir un niveau comparable de protection des données, notamment parce que la Knox Bill protège moins bien les droits de la personnalité, la communication de données personnelles aux Etats-Unis sera illicite.

6. Communication de données personnelles

6.1. Tribunal pénal international pour l'ex-Yougoslavie

Invité par le Tribunal Pénal International pour l'ex-Yougoslavie (TPIY) à établir une procédure d'identification de témoins potentiels des événements du Kosovo, le Département fédéral des affaires étrangères (DFAE) nous a consulté sur les aspects de protection des données à prendre en compte. Nous avons proposé la mise en place d'un processus basé sur le libre consentement des personnes à fournir des informations les concernant et sur la confidentialité des données fournies. Sur la base de nos considérations, le DFAE a transmis au TPIY une réponse positive quant à sa collaboration tout en tenant compte des exigences de la protection des données.

Saisi en avril 1999 d'une demande du Tribunal Pénal International pour l'ex-Yougoslavie (TPIY) d'établir une procédure d'identification de témoins potentiels des événements du Kosovo, le Département fédéral des affaires étrangères (DFAE) nous a consulté sur les aspects de protection des données à prendre en compte, notamment en ce qui concerne la distribution et la collecte de questionnaires auprès de personnes originaires du Kosovo. En effet, dans le cadre de sa demande, le TPIY a invité les autorités suisses à établir auprès des réfugiés kosovars accueillis dans notre pays une procédure d'identification de témoins directs des crimes commis au Kosovo en leur distribuant un questionnaire destiné à réunir des éléments de preuve nécessaires au TPIY pour juger les personnes responsables de violations graves du droit humanitaire.

Du point de vue de la protection des données, la clef de voûte du processus à envisager est le libre choix des personnes concernées à remplir et renvoyer au TPIY le questionnaire qui leur sera remis, et partant à fournir des données personnelles les concernant. Un complément indispensable à ce consentement sera l'information qui sera donnée à ces personnes, en particulier sur le but du questionnaire et sur leur libre choix à le remplir. Un tel procédé basé sur le consentement des personnes à fournir des informations les concernant permettrait en outre également de régler le fait de faire appel à la collaboration d'organismes de coordination en matière d'asile susceptibles de porter assistance aux personnes qui souhaitent remplir le questionnaire. Dans ce contexte de libre participation, le renvoi des questionnaires remplis au TPIY pourrait également être laissé au soin des personnes concernées qui pourraient, le cas échéant, le faire avec l'aide de ces organismes d'entraide. Une collecte par l'ODR des questionnaires remplis serait au demeurant envisageable à condition que celle-ci soit effectuée à seule fin de les transmettre de manière centralisée au TPIY.

Nous avons donc soutenu la démarche envisagée visant à confier à l'ODR la distribution de ce questionnaire, lequel serait accompagné d'une feuille explicative du DFAE concernant le but de la démarche, le libre consentement des intéressés à le remplir et, le cas échéant, la manière de le retourner au TPIY. Nous avons par contre indiqué également que des problèmes de protection des données devront être relevés s'il est envisagé de mettre en place un processus impliquant que les questionnaires une fois remplis soient récoltés et que, avant d'être transmis au TPIY, des copies soient effectuées et traitées par d'autres autorités tels que par exemple l'Office fédéral de la police ou l'Office de l'auditeur en chef. Une telle démarche ne répondrait en effet plus aux principes de finalité et de légalité. Elle sortirait de plus du cadre de la demande spécifique déposée par le TPIY.

Tenant compte de notre prise de position, le DFAE a transmis une réponse à l'attention du TPIY précisant que le gouvernement suisse, comprenant l'importance que revêt ce questionnaire pour les instigations menées par le TPIY, a décidé de lui prêter assistance en faisant remettre ledit questionnaire aux ressortissants kosovars arrivés en Suisse et tombant sous le mandat du TPIY. Le DFAE a de plus précisé que conformément à la législation fédérale sur la protection des données, le questionnaire sera rempli uniquement sur une base volontaire et confidentielle par les personnes concernées et qu'il sera envoyé par leurs soins directement au TPIY à La Haye. Ce dernier a transmis au DFAE ses remerciements pour la solution de collaboration proposée et sa parfaite compréhension pour le caractère volontaire et confidentiel à l'égard des personnes concernées du processus choisi.

6.2. Communication de l'identité de contrevenants au code de la route à des autorités étrangères

Qui n'a pas déjà mal garé sa voiture ou roulé trop vite à l'étranger ? La question se pose dans ce contexte entre autres de savoir si les autorités suisses sont autorisées à communiquer à des organes de police étrangers l'identité d'un contrevenant sur la base d'une plaque d'immatriculation suisse.

Nous avons à plusieurs reprises été contacté par des personnes ayant reçu par la poste une contravention délivrée par une autorité de police étrangère nous demandant par quel moyen cette autorité avait réussi à obtenir leur adresse, si cette démarche était légale et finalement s'ils devaient donner suite à cette décision.
Selon la loi sur la protection des données, les organes fédéraux ne sont en principe autorisés à communiquer des données personnelles à des tiers que si une

base légale suffisante existe à ce sujet ou si le destinataire a, en l'espèce, absolument besoin de ces données pour l'accomplissement de sa tâche légale (Art. 19 al. 2 LPD). Dans tous les autre cas, il est nécessaire d'obtenir le consentement de la personne concernée.
Dans la mesure où la Suisse a conclu un accord d'entraide judiciaire en matière pénale avec l'Etat étranger concerné – ce qui est le cas pour tous nos pays limitrophes – l'exigence d'une base légale suffisante est satisfaite et aucune objection ne peut donc être faite d'un point de vue de la protection des données contre la communication de l'adresse.
La base légale doit préciser quelle autorité suisse est en droit de communiquer à quelle autorité étrangère quelles données et pour quelles finalités.
Quant à la question de savoir si la contravention a été délivrée à bon droit ou à tort, elle ne relève pas du domaine de la protection des données, mais doit être examinée suivant la législation routière et les normes pénales applicables.

7. Le principe de transparence

7.1. Le principe de transparence et la protection des données

L'information et la communication constituent deux caractéristiques essentielles de cette fin de siècle. A l'aube du XIXe siècle, la société de l'information est devenue une réalité pour chacun d'entre nous. Si par le passé, le culte du secret et le règne de la non-transparence ont dominé nos sociétés, nous assistons à un renversement de tendance. L'administration devient plus transparente et les individus jouissent du droit au respect de leur vie privée. La liberté d'accès à l'information et aux documents administratifs ainsi que le droit à la protection des données sont deux impératifs démocratiques, nécessaires à l'avènement d'une société de l'information qui soit proche des citoyens. En Suisse, un projet de loi sur la transparence des documents administratifs est en consultation. En outre, lors de leur 6e conférence nationale, les commissaires suisses à la protection des données ont entamé le débat sur la relation entre protection des données et transparence.

De nombreux pays connaissent le principe de transparence (notamment l'Australie, la Belgique, le Danemark, la Finlande, la France, les Etats-Unis et le Canada). Le pionnier est la Suède qui l'a introduit, il y plus de deux cents ans. De même, nombreux sont les Etats, en particulier en Europe (notamment les 15 membres de l'Union européenne, la Norvège, l'Islande, la Pologne et la Slovénie) qui ont adopté des lois de protection des données. La Hongrie et le

Québec ont adopté des lois qui régissent l'accès à l'information et la protection des données. En Suisse, les premières lois de protection des données ont été adoptées à la fin des années 70. Aujourd'hui au côté de la Confédération, 17 cantons ont une loi. Par contre, l'introduction du principe de transparence n'en est encore qu'à ses premiers pas. Seul le canton de Berne s'est doté d'une loi. Toutefois, des travaux législatifs sont en cours. La Confédération prépare une loi, actuellement en procédure de consultation, et plusieurs cantons, dont Genève et le Tessin, ont également des projets. Le canton de Soleure envisage d'adopter une loi qui régira la protection des données et l'accès aux documents administratifs.

L'introduction du principe de transparence dans l'administration fédérale entraînera un changement de culture administrative. Aujourd'hui, la règle du secret prédomine et l'accès demeure l'exception. Avec l'adoption du projet de loi, actuellement en consultation, toute personne aura le droit d'accéder aux documents officiels sans avoir à justifier d'un intérêt et en principe gratuitement. La transparence ne sera pas totale et des exceptions seront possibles. En particulier, l'accès pourra être limité, différé ou refusé si un intérêt public ou privé prépondérant s'y oppose. Un intérêt public prépondérant au maintien du secret existera lorsqu'un document officiel porte notablement atteinte à la libre formation de l'opinion et de la volonté de l'autorité ou met en danger la sûreté intérieure ou extérieure de la Suisse. Il y aura un intérêt privé prépondérant à ne pas accorder l'accès lorsque le document est susceptible de porter notablement atteinte à la vie privée, de révéler des secrets professionnels, de fabrication ou d'affaires ou de divulguer des informations fournies librement par un tiers à l'autorité avec l'assurance de demeurer secrètes. Il n'y aura également pas d'accès aux documents officiels relatifs à la procédure de co-rapport et aux positions de négociation concernant des négociations internationales en cours ou futures. En ce qui concerne l'accès à des documents officiels, contenant des données personnelles, il demeure régi par la loi fédérale sur la protection des données. Cela ne veut pas pour autant dire que tout document contenant des données personnelles sera soustrait au principe de transparence. L'autorité pourra rendre un document accessible après l'avoir rendu anonyme (notamment caviardage ou recours à un pseudonyme). Le Préposé fédéral à la protection des données pourra également recommander la communication du document si l'intérêt public à la transparence l'emporte sur l'intérêt au maintien du secret, même si les conditions prévues par la LPD pour la communication des données ne sont pas remplies. Enfin, tout document mentionnant le nom d'une ou de plusieurs personnes n'est pas, pour ce seul motif, un document contenant des données personnelles. Il faut que les informations se réfèrent à une ou plusieurs personnes identifiées ou identifiables, qu'elles portent notamment une appréciation ou un jugement de valeur les concernant ou qu'elles incluent la description de leur comportement.

Le projet de loi met également en place un mécanisme en cas de conflit entre l'administration et l'administré souhaitant obtenir l'accès à un document officiel. Il est prévu une procédure de médiation avec un médiateur indépendant. En cas d'échec de la médiation, l'administré pourra obtenir une décision qu'il pourra, le cas échéant, porter devant la Commission fédérale de la protection des données et de la transparence. Lorsque le conflit porte sur un document contenant des données personnelles, la médiation sera assurée par le Préposé fédéral à la protection des données.
Entre le principe de transparence qui, par essence, postule l'ouverture et la protection des données qui garantit le respect de la vie privée des personnes au sujet desquelles des données personnelles sont traitées, il peut y avoir des tensions qu'il convient d'éliminer. Ces deux droits sont d'égale valeur et nous devons parvenir à un équilibre entre eux. Il ne doit pas y avoir opposition, mais complémentarité de deux impératifs démocratiques. Il faudra, en particulier, apprécier de cas en cas si l'intérêt à la transparence l'emporte sur le respect de la sphère privée ou si le maintien de la confidentialité s'oppose à la divulgation des informations. Ces deux droits ne sont pas absolus et il est nécessaire de vérifier par une pondération d'intérêts si les avantages offerts par l'un priment les inconvénients et les risques liés à l'autre. Dans nos sociétés, le fonctionnement de la démocratie implique parfois que certaines données personnelles traitées par des organes publics soient accessibles à tous et puissent être contrôlées. L'exigence de transparence et le droit de l'individu à l'accès aux documents officiels sont aussi motivés par les risques que nous font courir les technologies de l'information et de la communication. Le principe de la transparence se veut aussi un garde-fou face aux multiples traitements de données effectués par les administrations et qui mettent en danger le droit à la sphère privée.

Le Préposé fédéral à la protection des données est favorable à l'adoption d'une loi fédérale sur la transparence de l'administration qui contribuera à renforcer le processus démocratique et la confiance de l'administré dans l'administration. Il a jugé le projet actuel équilibré, même si certaines restrictions au droit d'accès sont trop absolues. Il est en outre favorable à l'institution d'un médiateur. Il estime toutefois qu'il serait préférable de lui confier également cette fonction vu la similarité des tâches et des questions abordées et du fait que des conflits surgiront fréquemment en présence de demandes d'accès à des documents contenant des données personnelles. Cette solution adoptée au Québec a débouché sur des résultats très positifs et permet une meilleure pondération des intérêts en présence. En outre, elle est plus économique. Le Préposé fédéral à la protection des données n'exclut pas qu'il soit nécessaire dans un avenir plus ou moins proche de rassembler les deux lois. Enfin, il rend attentif au risque qu'en l'absence de garanties appropriées, le principe de transparence ne favorise la commercialisation des données et ne débouche sur une plus grande diffusion au travers de l'Internet au détriment du respect de la sphère privée.

La consultation sur le projet de loi a démarré le 19 avril 2000.

8. Protection des données et conditions légales cadres

8.1. Les critères d'efficacité des codes de conduite en matière de protection de la sphère privée

Les codes de conduite ont désormais leur place dans le commerce électronique, parallèlement aux réglementations juridiques. Il ne s'agira donc pas à l'avenir de se demander si l'on doit les remplacer par des lois. Au contraire, il faudra créer un contexte dans lequel ceux-ci garantissent aussi à l'utilisateur et au consommateur une protection efficace de la sphère privée.

Certes, les codes de conduite sont susceptibles de promouvoir la relation de confiance. Mais ils ne peuvent remplacer les lois. Ils ne sont qu'un complément aux dispositions légales. Il convient donc d'œuvrer pour que ces codes de conduite contiennent au moins les éléments suivants:

- Une information claire et simple doit indiqué notamment le genre et la manière dont les données personnelles sont traitées.
- L'utilisateur doit avoir le choix quant à l'utilisation de ses données personnelles.
- Des mécanismes efficaces en matière de respect des droits de la personne concernée doivent être mis en place.
- Les critères de reconnaissance des codes de conduite (critères internationaux) doivent être uniformes.
- Les autorités et les milieux économiques doivent absolument être intégrés au processus de reconnaissance des codes de conduite.

Ces codes de conduite doivent contenir non seulement des informations sur le traitement des données, mais également des indications sur la livraison de la marchandise, le dédommagement éventuel ainsi que le for en cas de différend.

9. Protection et sécurité des données

9.1. La responsabilité de la direction des offices lors de projets informatiques

En principe, un projet informatique peut être subdivisé en plusieurs phases de planification et en une phase de réalisation. Le projet se termine une fois que le système a été mis en service auprès des utilisateurs. Suit alors l'exploitation du système avec les travaux de maintenance nécessaires. Lors de notre activité de conseil, nous avons pu constater qu'il existait des points faibles dans les phases de planification en ce qui concerne l'application des mesures de protection et de sécurité des données.

La sécurité des données peut en principe être décrite à l'aide des termes confidentialité, intégrité et disponibilité. Nous avons constaté que la disponibilité des systèmes ne pose aujourd'hui plus de problèmes majeurs pour autant que la fonctionnalité du système ne soit pas entravée par des virus ou par d'autres manipulations intentionnelles. La raison pour laquelle la disponibilité est aujourd'hui très haute est à notre avis due au fait que la non-disponibilité d'un système est immédiatement décelée par les organes directeurs. Ceci mène à ce que les organes directeurs prennent contact avec le responsable du service informatique pour examiner comment il est possible à l'avenir d'éviter de tels incidents. Dans les domaines de la confidentialité et de l'intégrité, la situation est plus complexe. Dans cet environnement, il est conseillé de s'assurer les services de consultants en matière de protection et de sécurité des données.
Un projet est toujours réalisé à l'aide d'une organisation de projet. Les responsables pour les questions de protection et de sécurité des données doivent être intégrés dans cette organisation de projet. Le projet proprement dit est en principe divisé en phases de planification (analyse préliminaire, conception) et en une phase de réalisation et de mise en œuvre conformément au standard HERMES (standard de l'administration fédérale pour la conduite et le déroulement de projets informatiques).
Dans les rapports « analyse préliminaire » et « conception » des indications doivent être fournies sur la protection ainsi que sur la sécurité des données. Nous avons constaté que dans un grand nombre de cas aucune indication n'était fournie pour satisfaire à ces exigences qualitatives. Les organes de direction n'attachent toujours pas assez d'importance à cet aspect. La protection et la sécurité des données doivent être prises au sérieux, discutées et appliquées au sein de l'organisation. La publication de violations en matière de protection ou de sécurité des données porte toujours atteinte à l'image de marque. Les organes de direction doivent veiller lors de projets informatiques à ce que les responsables pour la protection et la sécurité des données soient également impliqués dans les procédures de libération des phases « analyse préliminaire » et

« conception ». Un projet ne doit pas être poursuivi sans que ces instances aient donné leur feu vert pour entamer la phase suivante. A l'issue de la phase de conception, on élabore un cahier des charges. En fonction des coûts estimés du projet, ce cahier des charges est soit publié dans la Feuille officielle suisse du commerce, soit directement remis aux fournisseurs potentiels d'une solution. Ce cahier des charges doit contenir des indications sur les mesures relatives à la protection et à la sécurité des données.
Les mesures relatives à la protection et à la sécurité des données sont utilisés comme critères d'appréciation lors de l'évaluation des offres reçues. Ces critères représentent des conditions cadre et doivent donc être considérées comme objectifs impératifs. Ceci est surtout le cas lorsque cela concerne des données ou des systèmes sensibles.
Il incombe aux responsables de la protection et de la sécurité des données de veiller pendant la phase de réalisation à ce que les mesures prévues soient appliquées. Dans la phase d'exploitation, les mesures de protection et de sécurité des données doivent faire l'objet d'une surveillance périodique pour éventuellement demander des retouches.

9.2. L'application des prescriptions de la protection des données augmente la transparence et la gestion des unités administratives

La direction d'un office doit avoir un intérêt à ce que les processus d'accomplissement des tâches soient documentés et que l'on soit en mesure de déterminer quels moyens informatiques appuient quels processus. Sur la base de cette documentation, on peut comprendre à posteriori quelles informations ont été mises à disposition de quels exécutants pour quelles finalités.

Dans le domaine de la protection des données, il existe en principe trois types de processus. Il s'agit des processus d'accomplissement des tâches, d'information conformément au droit d'accès ainsi que des contrôles au sein d'un office.
Dans un système d'information du personnel par exemple, le processus d'accomplissement des tâches commence par la publication d'une annonce sur le marché de l'emploi suivi de la réception des dossiers de candidature et de leur examen par le service du personnel et ensuite de l'engagement d'un candidat et du renvoi des dossiers de candidature de ceux qui n'ont pas été retenus. Il y a lieu en outre de montrer les processus engagés par le service du personnel auprès des collaborateurs (tels que versement du salaire, promotions, etc.). Les processus doivent être mentionnés jusqu'à la fin du traitement des données afin de pouvoir vérifier à quel moment les informations ne sont plus

nécessaires (c.-à-d. qu'elles peuvent être supprimées) ou qu'elles doivent être transmises aux Archives fédérales.
En principe, cette documentation des processus doit montrer clairement quelles tâches sont exécutées et par quelles unités, quelles ressources matérielles (notamment informatiques) et quelles informations sont nécessaires pour accomplir les tâches.
Le processus du droit d'accès est la plupart du temps facile à décrire. Il s'agit de montrer qui traite la demande de renseignement et qui accomplit ensuite quelles activités permettant de trouver les dossiers et comment les documents sont mis à disposition du requérant et par l'intermédiaire de quelle instance.
Les processus de contrôle sont plus complexes. Il s'agit de montrer comment les responsables pour la protection et la sécurité des données assument leurs tâches. Les fonctions de contrôle des processus ou les processus de contrôle complets (tels que les procédures de modification, l'octroi des accès, les applications, le déroulement d'un contrôle au sein de l'office) doivent être décrits. Si ces processus sont documentés, on dispose d'une bonne vue d'ensemble de l'unité et on est en mesure de pouvoir constater à posteriori qui assume quelles tâches dans quels domaines (transparence dans l'unité administrative). Sans ces documents, il est difficilement possible de diriger une unité administrative. Pour des raisons qui relèvent de la protection et de la sécurité des données, le législateur exige en plus que la configuration des moyens informatiques ainsi que celle des mesures techniques et organisationnelles de sauvegarde des données soit documentée (voir aussi notre 5ème Rapport d'activités 1997/98, page 226). En fournissant la documentation mentionnée ci-dessus et en appliquant les mesures, les unités administratives remplissent les exigences de la loi sur la protection des données posées envers les personnes concernées et défendent les intérêts de la direction de l'office à disposer d'une gestion transparente et sûre de l'unité administrative.

9.3. Les dossiers de planification et de mise au concours de systèmes informatiques doivent impérativement inclure des mesures de protection des données

Suite aux phases de planification d'un projet informatique, on élabore un cahier des charges qui décrit les exigences envers le nouveau système informatique. Pour des systèmes sensibles, le cahier des charges doit contenir des exigences en matière de sécurité qui soient conformes au niveau technologique actuel. Nous avons constaté que nombre de fournisseurs renommés de solutions informatiques n'étaient pas en mesure de proposer des solutions de sécurité globales pour leurs systèmes. Nous devons d'autre part présumer que les cahiers des charges ne contiennent que très peu d'exigences

relatives à la sécurité des données et que souvent la sélection des systèmes se fait sans attacher l'importance nécessaire à cet aspect.

Du point de vue de la protection et de la sécurité des données, un cahier des charges doit contenir entre autres :

- l'exécution d'une analyse de processus permettant de constater qui (rôle) a besoin de quelles données sur la base de quelles tâches et pour quels buts (pour autant que cette tâche ne soit pas effectuée par des exécutants internes à l'unité administrative) ;
- les données doivent être cryptées lors de la transmission (y compris l'impression sur une imprimante réseau), à l'archivage ainsi que sur les bandes de sauvegarde (bandes backup);
- il y a lieu lors de l'identification et de l'authentification de prévoir une sécurité supplémentaire à l'identification de l'utilisateur (User ID) et du mot de passe, par exemple sous la forme de la présentation d'une carte à puces (personnelle) ou de la vérification des caractéristiques d'une personne (système biométriques);
- les traitements importants qui risquent de porter atteinte à la personnalité, doivent être journalisés de manière conforme aux exigences de la révision.

Nous avons interrogé des fournisseurs renommés de solutions informatiques pour savoir s'il existait une demande pour des mesures de sécurité, telles que des procédés de cryptage par exemple. La réponse fut que de telles exigences étaient plutôt rares, mais que l'on s'attendait à ce qu'elles augmentent à l'avenir. Le Préposé fédéral à la protection des données rend attentif depuis plusieurs années déjà au fait que des procédés de cryptage doivent être utilisés, particulièrement pour des systèmes sensibles. Les mesures de sécurité doivent faire partie intégrante des phases de planification et de réalisation d'un projet. Les conclusions tirées de ces phases de planification, notamment dans le domaine de la sécurité, doivent être intégrées dans une mise au concours ou un cahier des charges. La sélection des systèmes ne doit pas se faire uniquement sur la base des fonctionnalités, mais également en tenant compte des critères de sécurité. Les contraintes légales sont des objectifs d'ordre impératif; c'est la raison principale pour laquelle les mesures de sécurité dans un domaine sensible doivent être prises selon le niveau technologique le plus moderne. Les contraintes d'ordre normatif ne sont cependant souvent pas suivies. Nous rendons une fois de plus attentif au fait qu'une protection des données ne peut pas être garantie sans sécurité des données. En tant qu'organe de contrôle nous avons à plusieurs reprises déjà rendu attentif au fait qu'il était nécessaire d'agir.

9.4. Etat et application des mesures de protection et de sécurité des données en ce qui concerne le système d'information du personnel PISEDI

Les travaux concernant le système d'information du personnel PISEDI ont encore une fois pris du retard. Ceci est surtout dû à la charge de travail des informaticiens liée aux problème de l'an 2000, mais aussi à la réorganisation du secteur informatique de l'administration fédérale (NOVE-IT). Le Préposé fédéral à la protection des données a reçu le rapport final de sécurité au cours du troisième trimestre 1999. Pour pouvoir élaborer de manière définitive le règlement de traitement, il nous manque encore certains documents qui devraient être disponibles cette année encore.

Lors de nos entretiens avec les responsables du système PISEDI, nous avons rendu attentif au fait qu'il fallait prendre comme base pour l'application des mesures techniques et organisationnelles de sécurité des données le manuel n° 1 relatif à la directive n° S02 « Sécurité informatique » (voir également notre 6ème Rapport d'activités 1998/99, page 332). Par la suite, le système PISEDI a été analysé à l'aide du catalogue de mesures, respectivement de la check-list contenue dans la directive susmentionnée. Ceci a déjà permis d'améliorer la sécurité. Cependant, il existe encore des dérogations, notamment au niveau de la journalisation et dans l'usage des procédés de cryptage. La direction du DFI a réalisé qu'il était nécessaire d'agir et elle désire professionnaliser la sécurité informatique. Il est ainsi prévu d'inclure dans un règlement de traitement les principaux éléments qui à l'issue de cette analyse ont été identifiés comme jouant un rôle pour la sécurité. Il a donc été possible ainsi d'élaborer une nouvelle partie de ce règlement. Il manque cependant encore quelques autres parties qui devraient être documentées de manière définitive dans le courant de cette année.

10. Militaire

10.1. Affaire Bellasi: aspects relevant de la protection des données

Dans le cadre de « l'affaire Bellasi », nous avons pris position à l'attention de la Délégation des Commissions de gestion sur des critiques émises dans la presse à l'encontre de la protection des données limitant soi-disant les contrôles de sécurité. La Délégation a partagé notre opinion selon laquelle aucune exigence ou norme de protection des données n'a entravé l'exécution des contrôles de sécurité et que les nouvelles règles en la

matière ainsi que les dispositions spécifiques applicables au service de renseignements répondaient parfaitement aux besoins d'aujourd'hui. La Délégation a par contre relevé le caractère purement formel et superficiel de ces contrôles. Elle a recommandé au Conseil fédéral de réviser l'ordonnance y relative afin d'en améliorer les modalités d'exécution.

Dans le cadre de « l'affaire Bellasi », la Délégation des Commissions de gestion (DCG) a examiné les règles relatives au contrôle de sécurité des personnes. Or dans ce contexte, différents articles de presse ont fait référence au problème de la conservation des documents des contrôles de sécurité. Certains articles ont soutenu que des actes relatifs aux contrôles de sécurité dont a fait l'objet M. Bellasi ont été détruits après un délai de cinq ans, mettant ainsi en cause la prééminence de la protection des données au détriment des intérêts de l'Etat. Il nous est dès lors apparu important d'attirer l'attention de la DCG sur certains points à prendre en compte dans l'analyse de ces allégations.

Les examens de sécurité ont fait l'objet ces dernières années de nombreuses réglementations qui ont toujours tenu compte du caractère particulier que représentent le domaine militaire et la sécurité de l'Etat. La protection des données n'a jamais formulé d'exigences pouvant mettre en péril ces secteurs sensibles. Au début des années nonante (période au cours de laquelle certains documents relatifs au contrôle de sécurité effectué auprès de M. Bellasi sembleraient avoir été détruits) les ordonnances applicables en matière de contrôle de sécurité prévoyaient que l'organe de contrôle détruise les documents après cinq ans. Avec le consentement de la personne concernée, ces documents pouvaient être déposés aux Archives fédérales au lieu d'être détruits. En outre, pour les contrôles de sécurité dans le domaine militaire, il était prévu que les données soient conservées durant cinq ans et détruites ensuite. De plus, un procès-verbal de destruction devait être établi et conservé pendant dix ans. Enfin, pour de justes motifs, le chef de l'état-major général pouvait prévoir des exceptions à la durée de conservation. Dès lors, dans le cas d'espèce, aucune norme ou exigence de protection des données n'imposait la destruction d'actes issus de contrôles de sécurité. Au contraire, la réglementation en vigueur en matière de contrôle de sécurité contenait les garde-fous adéquats permettant de garantir la sécurité militaire et d'assurer les intérêts de l'Etat.

En outre, la Commission d'enquête parlementaire chargée en 1990 de clarifier les faits survenus au Département militaire fédéral avait relevé que les réglementations susmentionnées répondaient en grande partie aux exigences qu'elle avait formulées. Il a par contre été soutenu que les interventions de l'Etat dans les droits fondamentaux de la personnalité requièrent une base légale formelle et qu'une simple ordonnance ne suffisait pas. Les premières démarches en ce sens

débouchèrent sur l'élaboration d'une norme provisoire dans la loi fédérale sur l'armée et l'administration militaire. Une réglementation détaillée au niveau d'une loi au sens formel a finalement été introduite dans la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) entrée en vigueur le 1er juillet 1998.

Une nouvelle ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP) a été adoptée le 20 janvier 1999. Elle stipule que l'autorité requérante peut charger le service spécialisé de répéter le contrôle lorsqu'elle a des raisons de présumer qu'un risque nouveau pour la sécurité est apparu depuis le contrôle précédent ou lorsque des conventions internationales sur la protection des secrets le prescrivent. D'autre part en matière de conservation des données, non seulement cette dernière a été doublée, passant de cinq ans à dix ans, mais de plus la notion de destruction a été abandonnée. Il est ainsi prévu que le service spécialisé conserve les dossiers aussi longtemps que la personne concernée occupe la fonction considérée ou collabore à l'exécution du contrat mais au plus tard durant dix ans. Passé ce délai, il les propose aux Archives fédérales pour qu'ils soient archivés.

Il importe enfin de mettre en relief le fait que des normes complémentaires sont applicables au renseignement militaire. La loi fédérale du 3 février 1995 sur l'armée et l'administration militaire contient des dispositions spécifiques applicables au service de renseignements prévoyant que le Conseil fédéral règle le détail des tâches de renseignements, son organisation et la protection des données. Se fondant sur cette base légale spécifique, l'Ordonnance sur le renseignement du 4 décembre 1995 prévoit que le Service de renseignements peut recueillir, traiter et utiliser toutes les informations nécessaires, y compris celles qui concernent des personnes, afin notamment d'assurer le contrôle de sécurité relatif aux personnes qui travaillent ou travailleront pour lui.

Ainsi dans « l'affaire Bellasi », les normes applicables en matière de contrôles de sécurité contenaient tous les mécanismes adéquats permettant d'effectuer les contrôles nécessaires. Sur la base de ces considérations, nous avons rappelé que tant les anciennes que les nouvelles réglementations en matière de contrôle de sécurité ont constitué dans le cas d'espèce des bases légales adéquates garantissant les intérêts de l'Etat et de la sécurité militaire. Aucune règle de protection des données n'a remis en cause ces intérêts, ni limité la réalisation de contrôles de sécurité, ni imposé la destruction d'actes issus de tels contrôles. Nous avons conclu notre prise de position en relevant qu'aucune exigence ou norme de protection des données n'entravait donc l'exécution des contrôles de sécurité et que de notre point de vue les nouvelles règles spécifiques entrées en vigueur récemment en matière de contrôle de sécurité à l'égard d'agents de la Confédération, de militaires ou de tiers ainsi que les dispositions spécifiques en la

matière applicables au service de renseignements répondaient parfaitement aux besoins d'aujourd'hui.

La délégation des Commissions de gestion, partageant notre opinion, a repris différents extraits de notre prise de position dans son rapport du 24 novembre 1999 sur les « Événements survenus au groupe de renseignements de l'état-major général – affaire Bellasi ». Elle a toutefois précisé qu'il ne faut pas minimiser le fait que ces dispositions sont récentes et qu'elles sont loin d'avoir été assimilées dans l'administration. De plus, la DCG a également constaté que les examens de sécurité restent dans la réalité purement formels et superficiels. Dans son rapport, la DCG a conclu que si la législation paraît offrir les garanties nécessaires à la sauvegarde de la sécurité, les modalités prévues pour l'exécution de ces contrôles sont si restrictives qu'ils en perdent l'essentiel de leur crédibilité. La délégation a donc recommandé au Conseil fédéral de réviser l'ordonnance sur les contrôles de sécurité relatifs aux personnes afin de permettre une répétition régulière des contrôles, une utilisation plus large des enquêtes de police ou encore une répétition systématique des contrôles de sécurité lorsqu'une personne déjà contrôlée vient à assumer une nouvelle fonction aussi sujette à contrôle.

11. Archives

11.1. Ordonnance relative à la loi sur les archives

Après l'adoption de la loi fédérale sur les archives par les Chambres fédérales le 26 juin 1998, un projet d'ordonnance nous a été soumis pour examen. Nous avions participé au sein d'un groupe de travail interdépartemental à l'élaboration de ce projet.

Le projet prévoyait une modification de l'ordonnance sur la protection des données qui eut permis à tous les organes fédéraux de publier des listes avec des données personnelles dans la mesure où un intérêt public existait. A notre avis, il était inopportun de vouloir régler au sein d'une norme à caractère général des questions qui se posaient en première ligne dans le contexte de données archivées, notamment la question de l'admissibilité de la publication de ce que l'on appelle des inventaires et en particulier de listes nominatives (voir à ce sujet notre prise de position concernant l'interpellation Scheurer, 6ème Rapport d'activités 1998/99, pages 310 ss). A notre avis, une telle réglementation eût été en nette contradiction avec la volonté du législateur. L'article 19, al. 2 LPD stipule notamment que les organes fédéraux sont autorisés sur demande et dans des cas individuels à communiquer le nom, l'adresse ainsi que la date de nais-

sance d'une personne même en l'absence d'une base juridique au sens de l'article 17 LPD. Le législateur n'autorise donc pas, sans base juridique, la communication systématique, ni la publication de données personnelles, notamment sous forme de listes nominatives. De notre point de vue, rien ne s'opposait à la création d'une base légale qui eut permis aux Archives fédérales de publier certaines données personnelles sous forme de listes nominatives dès lors qu'un intérêt public existait, dans le but d'éclaircir certains événements et faits historiques. Une telle norme aurait cependant dû être intégrée dans l'ordonnance sur les Archives fédérales et non dans l'ordonnance relative à la loi fédérale sur la protection des données. La question de savoir s'il existe un besoin de donner également la possibilité à d'autres organes fédéraux de publier dans certaines conditions des données personnelles, notamment sous forme de listes, devrait encore être examinée. Pour ceci, une base légale au niveau d'une ordonnance ne suffirait certainement pas, étant donné que les informations devant être publiées contiennent sans aucun doute des données sensibles. Au vu de ces réflexions et afin de ne pas retarder l'entrée en vigueur de la loi sur les archives et de l'ordonnance respective, on a renoncé à la norme concernant la publication des listes. Pour les mêmes raisons, la décision a été prise de ne pas publier la liste des réfugiés ayant été accueillis en Suisse pendant la Seconde Guerre mondiale, mais d'ouvrir par contre au public l'accès aux archives pour la période concernée. Le 1er octobre 1999, la loi sur les archives et l'ordonnance d'exécution correspondante sont entrées en vigueur. On discute cependant la question de savoir si les organes fédéraux sont autorisés à publier des données personnelles. A l'occasion, il serait peut-être opportun de créer les bases légales nécessaires.

12. Secteur locatif

12.1. Traitement de données relatives à des locataires

Les bailleurs et les régies immobilières sont confrontés quotidiennement à de gros volumes de données concernant des locataires. La question de savoir si et dans quelle mesure des données personnelles peuvent être communiquées à des tiers ne trouve pas de réponse simple dans la pratique. Vous trouverez ci-dessous les réponses aux questions qui sont le plus souvent posées dans ce contexte.

Communication à des tiers de manière générale

Les données concernant les locataires servent en premier lieu à l'exécution du contrat de bail. Le bailleur n'est donc par principe pas autorisé à communiquer à

des tiers des données concernant un locataire sans le consentement de ce dernier. Une communication de données sans le consentement du locataire concerné ou contre sa volonté expresse (blocage) constitue une violation des droits de la personnalité au sens de la législation sur la protection des données. La communication des données est également inadmissible dans la mesure où il n'est pas justifié par un intérêt prépondérant privé ou public ou une disposition légale. Une communication sans motif justificatif constitue une violation du principe de la finalité et est donc contraire à la loi. Le bailleur est responsable des données concernant les locataires qui lui ont été confiées et est tenu pour le traitement de ces données de respecter les principes généraux de protection des données (licéité, bonne foi, proportionnalité, finalité, exactitude). Quant à la question de savoir si un intérêt public ou privé prédomine sur l'intérêt du locataire de ne pas divulguer ses données, elle doit être examinée de cas en cas en pesant les intérêts en présence.

Demandes de références

Les bailleurs ou régies immobilières sont souvent contactés par d'autres régies leur demandant des références sur des locataires actuels ou anciens. La question se pose de savoir si la personne sollicitée pour le renseignement est en droit de fournir des indications sur le locataire concerné et si oui, dans quelle mesure.
La demande de références de la part du bailleur potentiel nécessite l'accord du locataire intéressé (voir aussi notre aide-mémoire concernant les formulaires d'annonce pour appartements à louer qui peut être obtenue auprès du PFPD ou accessible sur le site www.edsb.ch). La personne sollicitée pour fournir une référence n'est en droit de donner le renseignement que si le locataire concerné a expressément indiqué cette personne comme référence. Ceci signifie que les bailleurs actuels ou précédents ne peuvent pas automatiquement être considérés comme références. En cas de doute, il est judicieux de s'assurer auprès du locataire concerné si celui-ci a vraiment donné son accord ou non. Le droit à l'information doit en outre être restreint à la confirmation des indications faites sur le formulaire pour locataires potentiels. Quant à la question de savoir quelles informations peuvent être fournies concernant des locataires potentiels, nous renvoyons à l'aide-mémoire du PFPD cité ci-dessus.

Tenue de «journaux de conflits»

Nombre de régies immobilières tiennent ce que l'on appelle des «journaux de conflits» concernant des litiges intervenus avec des locataires. Pour autant qu'il s'agisse de régies immobilières employant un certain nombre de collaborateurs, la question se pose de savoir à qui ces dossiers ou informations peuvent être communiqué et dans quelle mesure.
Respectant les principes de la proportionnalité et de la finalité, nous défendons le point de vue que seules les personnes qui sont vraiment impliquées dans un

conflit doivent avoir accès à de telles informations. Ceci doit en outre n'être le cas que dans la mesure où ces personnes ont vraiment besoin de ces informations pour accomplir leur tâche. Dans ce contexte, la règle de base est: le moins de données possible, seules les données qui sont vraiment nécessaires; ceci d'autant plus que cela risque dans le cas précis de concerner des données sensibles ou des profils de la personnalité au sens de la législation sur la protection des données. En ce qui concerne la communication ou la transmission de données à des tiers, ce qui a été dit dans le paragraphe respectif est applicable de manière analogue.

13. Associations

13.1. Aide-mémoire concernant le traitement d'adresses de membres d'une association

Etant donné que les demandes en rapport avec le traitement de données concernant des membres d'une association se sont récemment multipliées, nous avons trouvé qu'il était judicieux de rédiger un aide-mémoire sur ce sujet. Vous trouverez cet aide-mémoire à la page 247 du présent rapport.

14. Divers

14.1. Commercialisation d'un CD-ROM concernant des données relatives aux détenteurs de véhicules: violation de l'interdiction d'exploitation prononcée par la Commission fédérale de la protection des données

Après avoir constaté à plusieurs reprises que l'interdiction d'exploitation prononcée contre le CD-ROM AUTOdex avait été violée, la Commission fédérale de la protection des données a rendu, à notre demande, le 16 février 1999 une décision exécutoire (cf. 6ème Rapport d'activités 1998/99, p. 335). La firme qui a produit le CD ne s'est pas conformée à cette décision. Les autorités judiciaires compétentes ont prononcé une amende contre la firme en question.

En 1998, la Commission fédérale de la protection des données (CFPD) avait déjà rendu une décision ordonnant la cessation définitive de la production et de la diffusion du CD-ROM AUTOdex contenant des données relatives aux détenteurs de véhicules en Suisse. Cette décision n'a pas été respectée par l'entreprise responsable. Au contraire, une nouvelle version du CD-ROM a été

mise sur le marché. Nous avons donc demandé à la CFPD de rendre une décision exécutoire, ce qu'elle a fait le 16 février 1999, interdisant donc à l'entreprise responsable de continuer à produire et à diffuser le CD-ROM AUTOdex sous menace expresse de suites pénales prévues par l'art. 292 du Code pénal suisse (CP). Nous avons appris par la suite que l'entreprise en question continuait à diffuser le CD-ROM sur commande. Nous avons dénoncé à l'autorité judiciaire compétente l'entreprise en question pour violation de la décision exécutoire de la CFPD. Par décision du 9 novembre 1999, la firme responsable a été condamnée à une amende.

III. ACTIVITÉS INTERNATIONALES

1. Conseil de l'Europe

- Travaux du CJPD: adoption du projet de recommandation sur les assurances

Le Groupe de projet sur la protection des données (CJPD) a adopté un projet de recommandation régissant la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

Le Groupe de projet sur la protection des données (CJPD) s'est réuni à une seule reprise, du 12 au 15 octobre 1999. Il a terminé l'examen du projet de recommandation sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance. Ce texte, qui devrait prochainement être adopté par le Comité des Ministres, régit l'ensemble des opérations de collecte et de traitement de données à caractère personnel liées à la couverture d'un risque, notamment en vertu d'un contrat ou d'une police d'assurance. Il ne couvre en principe pas les traitements de données effectués dans le cadre de la sécurité sociale. Le projet de recommandation précise notamment les conditions de licéité du traitement de données à des fins d'assurance, précise les finalités pour lesquelles de telles données peuvent être collectées et traitées, régit les droits des personnes concernées (en particulier droit à l'information et droit d'accès), fixe le cadre dans lequel des décisions individuelles automatisées peuvent être prises à des fins d'assurance, précise les obligations de sécurité et règle les flux transfrontières de données. Ce texte, à l'élaboration duquel nous avons étroitement collaboré, répond aux exigences du droit européen et notamment de la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le CJPD a en outre adopté un avis à l'intention du Comité des Ministres sur la Recommandation

1402 (1999) de l'Assemblée parlementaire relative au contrôle des services de sécurité intérieure dans les Etats membres du Conseil de l'Europe.

- Travaux du T-PD: protocole additionnel, données sensibles et clauses contractuelles

Le Comité consultatif de la Convention pour la protection des données à l'égard du traitement automatisé des données à caractère personnel (T-PD) a tenu sa 15e réunion du 16 au 18 juin 1999. Il a en particulier adopté un projet de protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données. Ce projet fera l'objet d'un avis de l'Assemblée parlementaire avant son adoption par le Comité des Ministres.

Ce projet de protocole complétera la Convention 108 sur deux points. Il prévoit l'obligation pour les Parties d'instituer une ou plusieurs autorités de contrôle exerçant leurs fonctions en toute indépendance. Cette autorité de contrôle doit être chargée de veiller au respect des dispositions de protection des données. Elle doit être dotée de pouvoir d'investigation et d'intervention. Elle doit pouvoir ester en justice ou porter à la connaissance d'une autorité judiciaire les violations qu'elle aura constatées. Le protocole régira également la communication transfrontière de données personnelles vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention. Il prévoit en particulier que la communication ne peut avoir lieu que si un niveau de protection adéquat est assuré pour le transfert considéré. Ce protocole doit permettre un renforcement des principes de la Convention 108 et contribuer à améliorer la protection effective des droits garantis par cette Convention. Il tient compte de l'évolution du droit et notamment de la directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Le Comité consultatif a également commencé une étude sur les données sensibles et élaboré un questionnaire qui a été adressé à l'ensemble des Etats membres du Conseil de l'Europe. Cette étude a pour objectif d'évaluer la manière dont les différents Etats membres ont réglé la question des données sensibles dans leur législation nationale et de mieux connaître l'interprétation qui a été donné des différents termes de la définition de données sensibles. Elle devrait permettre de déterminer si le concept de données sensibles doit être revu et si notamment le catalogue doit être étendu. Enfin, le Comité consultatif a entamé la révision des clauses contractuelles types de 1992 visant à assurer une

protection équivalente des données dans le cadre des flux transfrontières de données.

- Projet de Protocole sur la génétique humaine

Ce projet de protocole additionnel à la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine (Convention d'Oviedo) a été initialisé en novembre 1997. Le groupe de travail chargé de ce projet est composé de membres du Comité directeur pour la bioéthique, enrichi de spécialistes en génétique, santé, théologie et protection des données.

Les 2e et 3e réunions du groupe de travail se sont déroulées du 13 au 15 janvier 1999, et du 25 au 27 octobre 1999 à Strasbourg. Un projet de structure du protocole a été esquissé, prévoyant des dispositions générales, des normes relatives aux applications de la génétique dans les domaines de la santé et hors de ces domaines, à savoir en particulier à des fins d'assurance, d'emploi et d'identification. Il est également prévu d'intégrer à ce document des dispositions relatives au consentement, ainsi qu'un chapitre «protection de la vie privée et information du public». Actuellement, le groupe concentre ses travaux sur les dispositions générales et le chapitre relatif aux applications dans les domaines de la santé. Ces derniers recouvrent aussi bien les tests individuels que les dépistages, la thérapie génique, la recherche et le conseil génétique.

Des réflexions ont été menées sur l'opportunité de faire figurer les définitions dans le rapport explicatif du protocole, afin de pouvoir les réviser plus rapidement et de mieux tenir compte de l'évolution fulgurante en matière de génie génétique. Nous avons considéré que cette solution ne pouvait être acceptable qu'à la condition que l'adaptation des définitions n'implique pas de modification du champ d'application, du sens ou de la portée du protocole.

Des propositions ont en outre été faites au sein du groupe de travail pour atténuer l'importance de la protection de la personnalité des patients au profit d'autres intérêts, tels ceux de la recherche ou du commerce de tests génétiques sur Internet.

- Séminaire du Conseil de l'Europe: développement du droit de la protection des données dans le secteur de la police

Le Conseil de l'Europe a organisé en décembre 1999 un séminaire sur le thème de la «protection des données dans le secteur de la police». Participant à ce séminaire à Strasbourg, nous avons ainsi eu l'occasion d'examiner avec d'autres experts européens

les différentes réglementations nationales et internationales en matière de traitement de données personnelles face aux des développements des techniques toujours plus performantes de recherches policières. Une série de recommandations visant à une adaptation de certaines normes de protection des données a été élaborée à l'issue des débats.

En décembre 1999, nous avons participé au séminaire « protection des données dans le secteur de la police » organisé à Strasbourg par le Conseil de l'Europe dans le cadre du programme relatif aux activités pour le développement et la consolidation de la stabilité démocratique. Ce séminaire avait pour but de rappeler les principes fondamentaux de la protection des données dans le secteur de la police tels qu'ils ressortent notamment des dispositions de la Convention no 108 du Conseil de l'Europe sur la protection des données à caractère personnel, de la Recommandation R (87) 15 sur l'utilisation des données à caractère personnel dans le secteur de la police ainsi que des législations nationales et internationales.

Sur la base de ces réglementations, les experts spécialisés dans la protection des données participant au séminaire ont procédé à un échange de vues et d'expériences sur différents thèmes tels que les délais de conservation d'informations criminelles, l'utilisation de données collectées sur des personnes tierces non directement suspectes dans le cadre d'une enquête pénale, la notification des personnes dont les données ont été conservées à leur insu par la police, la conservation et l'utilisation de données génétiques en vue de l'identification de criminels ou encore l'établissement d'autorités de contrôle chargées de veiller au respect de la protection des données personnelles dans le domaine la police. En complément à ces discussions, différents instruments et cadres juridiques internationaux de coopération policière tels qu'Interpol, Europol ou Schengen ont fait l'objet d'exposés et de débats.

En conclusion à ce séminaire, les experts ont adressé différentes recommandations à l'attention notamment des législateurs nationaux afin de réglementer dans le droit interne les questions soulevées par les développements de la criminalité, les besoins et les méthodes de la police en regard des exigences de la protection des données. Il a ainsi été recommandé que face aux flux croissants des communications internationales des informations de police, les Etats garantissent une évaluation sérieuse de la qualité des données personnelles communiquées, un contrôle efficace des fichiers de police ainsi qu'une assistance effective aux personnes concernées même au-delà des frontières nationales.

Les participants ont également appelé à davantage de concertation et de coopération au niveau international. Ils ont exprimé le souhait que le Conseil de l'Europe poursuive l'examen des questions soulevées à l'occasion de ce

séminaire et étudie la possibilité d'élaborer des instruments juridiques complémentaires afin de promouvoir et renforcer la protection des données personnelles. Dans cette optique, il a été notamment proposé que soit examinée l'opportunité d'élaborer une recommandation additionnelle à la Recommandation R (87) 15 sur l'utilisation des données à caractère personnel dans le secteur de la police. Une telle démarche permettrait ainsi de prendre en compte les nouveaux moyens de collecte de données de police, les traitements toujours plus performants et intensifs des informations criminelles, l'usage de nouvelles méthodes et techniques de recherches policières (vidéosurveillance, Internet, collecte de données génétiques, enregistrement de personnes tierces) ou encore l'accroissement des échanges transfrontaliers de données de police.

2. Relations avec l'Union européenne

- Niveau de protection des données adéquat reconnu à la Suisse

Aux termes de l'article 25 de la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le transfert de données vers des pays tiers ne peut en principe avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. La Commission devrait reconnaître à la Suisse un niveau de protection adéquat en raison de sa législation interne et des ses engagements internationaux.

Le niveau adéquat est en principe apprécié pour chaque transfert. Il peut également faire l'objet d'une appréciation globale sur la base d'un examen de la législation interne et des engagements internationaux des Etats tiers en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. La Commission examine actuellement la législation de plusieurs Etats tiers et notamment celle de la Suisse. Après avoir été entendu par les services de la Commission (voir notamment 6ème Rapport d'activités 1998/99, p. 342ss.) et avoir répondu par écrit aux questions du Groupe de protection des données à l'égard du traitement de données à caractère personnel mis en place par la directive, celui-ci a rendu un avis favorable à notre égard (voir Avis 5/99 concernant le niveau de protection des données à caractère personnel en Suisse**,** http://www.europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs/index.htm).
Bien que la situation dans les cantons soit encore insatisfaisante (seuls 17 cantons ont des dispositions de protection des données dans une loi au sens formel), le Groupe a tenu compte de différents éléments pour proposer de reconnaître un niveau de protection adéquat également à l'ensemble des cantons. Il a en particulier tenu compte du fait que :

- les législations adoptées par les cantons s'inspirent largement de la Convention 108;
- les traitements de données à caractère personnel doivent répondre aux principes généraux découlant de la jurisprudence du Tribunal fédéral;
- même en l'absence de dispositions cantonales de protection des données, le traitement de données personnelles effectué par des organes cantonaux en exécution du droit fédéral est soumis à la loi fédérale sur la protection des données;
- pour les traitements effectués par des organes cantonaux en exécution du droit fédéral, les cantons doivent disposer d'un organe de surveillance chargé du respect de la protection des données et doté des mêmes compétences que le Préposé fédéral à la protection des données;
- certains traitements sont soumis à des normes spécifiques de confidentialité.

Sur cette base, la Commission devrait prochainement rendre une décision favorable à la Suisse. Une telle décision ne dispense pas les cantons qui n'ont pas encore adopté de loi sur la protection des données de légiférer sans attendre. En effet, avec l'entrée en vigueur de la nouvelle Constitution fédérale qui reconnaît à toute personne le droit d'être protégée contre l'emploi abusif des données la concernant, chaque canton a l'obligation de prendre les mesures nécessaires à rendre effectif ce droit. Il doit notamment adopter une loi de protection des données et mettre en place une autorité de contrôle dotée de moyens suffisant à l'accomplissement de ses tâches. Si certains cantons s'abstenaient d'agir, le législateur fédéral devrait étudier la possibilité d'étendre, à titre subsidiaire, l'application de la loi fédérale aux cantons sans législation offrant un niveau de protection des données suffisant.

3. Conférence internationale des commissaires à la protection des données

La XXIe Conférence internationale des commissaires à la protection des données s'est déroulée à Hong-Kong du 13 au 15 septembre 1999. Cette conférence réunissait les commissaires à la protection des données de 25 Etats du monde entier, des experts gouvernementaux, des représentants de l'OCDE et de l'Union européenne, ainsi que de l'industrie et de la science. A son terme et sur notre proposition, la Conférence a adopté une déclaration se référant aux recommandations du Groupe de protection des données à l'égard du traitement de données à caractère personnel mis en place par la directive européenne et au rapport présenté par la Commission nationale de l'informatique et des libertés (France). Cette déclaration invite les gouvernements à limiter la durée de

conservation des données de trafic en matière de télécommunication, laquelle devrait être la plus courte possible et à respecter le droit des personnes lors de la communication de ces données à un tiers.

La Conférence a abordé le problème des technologies de l'information à l'heure de la globalisation et du commerce électronique (http://www.pco.org.hk/conproceed.html). Elle s'est en particulier penchée sur les risques et les avantages des technologies pour la vie privée, sur la manière d'assurer la vie privée dans un environnement globalisé, sur les dangers de la surveillance et sur la sécurité des données dans le cadre de «révisions vie privée». Elle a abordé également le problème de la coopération internationale en matière de police, la relation entre la liberté d'information et la protection des données, la protection des données dans les nouveaux médias et les implications pour la protection des données de l'émergence d'une cyber-législation, ainsi que la question des droits des consommateurs face au commerce électronique. La Conférence a également créé un groupe de travail chargé d'évaluer la possibilité pour les commissaires à la protection des données de mettre en place des procédures de «certification protection des données».

En marge de la Conférence internationale, s'est également tenue la Conférence des commissaires européens à la protection des données qui regroupent les commissaires des pays membres de l'Union européenne et de l'Espace économique européen. Nous y avons participé pour la première fois avec le statut d'observateur. La Conférence a dressé un bilan des actions qu'elle a entreprises et dégagé les priorités pour l'année en cours. Elle a également mis l'accent sur l'importance de la formation et de la sensibilisation dans le domaine de la protection des données, sensibilisation qui doit débuter dans les écoles.

4. OCDE

- Groupe de travail sur la sécurité de l'information et la protection de la sphère privée

Au cours de l'année écoulée, le Groupe de travail sur la sécurité de l'information et la protection de la sphère privée (WISP) a concentré ses activités sur la recherche de solutions contractuelles applicables aux transmissions de données à l'étranger, sur la mise au point d'un générateur de déclaration de politique de la vie privée sur Internet et, enfin, sur l'uniformisation des techniques dans le domaine des signatures digitales.

- Contrats relatifs aux transmissions de données à l'étranger

Les Etats membres du groupe de travail estiment nécessaire de jeter des ponts entre les différents systèmes légaux de protection de la sphère privée. Ces contrats sont à ce propos un moyen permettant de garantir une protection adéquate au-delà des frontières.

Au cours des différentes discussions, nous avons émis les remarques suivantes :
- Face aux problèmes que posent les différents systèmes juridiques en matière de protection des données, les contrats peuvent constituer un début de solution afin de protéger, à l'étranger aussi, la sphère privée des citoyens.
- A cet effet, l'OCDE doit coopérer avec d'autres organisations internationales (Conseil de l'Europe, Union européenne).
- Les solutions contractuelles ne seront valables que si elles sont véritablement efficaces, c'est-à-dire si la sphère privée des personnes concernées est réellement protégée.
- Les travaux de l'OCDE doivent surtout mettre l'accent sur l'élaboration de critères permettant de garantir l'efficacité de la protection de la sphère privée sur la base de contrats.

Sur mandat du secrétariat du Groupe de travail WISP, une étude comparative sur les contrats applicables aux transmissions de données à l'étranger a été élaborée. Arguant de la liberté contractuelle régnant à propos du droit applicable en cas de litige, les Etats-Unis ont demandé la suppression de plusieurs paragraphes de cette étude. Dans ce contexte, nous avons souligné qu'en Suisse, la protection de la sphère privée est un droit fondamental inscrit dans la Constitution. Il est donc impossible d'affaiblir la garantie constitutionnelle de la protection de la sphère privée par des accords contractuels. Nous demandons que les passages du rapport concernant les limites de la liberté contractuelle ne soient pas biffés.
La question du droit régissant ces conventions contractuelles ne doit pas se traduire, en Suisse, pour une personne morale ou physique désirant ou devant transmettre des données personnelles à l'étranger, par l'obligation d'abandonner des droits garantis par la Constitution.

- Générateur de déclaration de politique de la vie privée de l'OCDE

Ainsi que le secrétariat du Groupe de travail pour la sécurité de l'information et la protection de la sphère privée l'avait déjà annoncé l'an dernier, une solution technique – le générateur de l'OCDE – permet désormais de générer automatiquement sur Internet des déclarations types de traitement de données. Le but de ce projet est de promouvoir les mesures et déclarations protégeant la sphère privée dans les transactions en ligne.

Ce générateur permet aux prestataires de garantir la transparence des traitements de données qu'ils effectuent sur Internet. Il contient en outre des instructions sur l'application des directives de l'OCDE pour la protection de la sphère privée sur Internet.

Nous avons fait observer que le générateur de l'OCDE peut être mis à profit utilement pour la formation et l'éducation. Les entreprises présentes sur Internet sont ainsi à même de pratiquer une politique en matière de traitement des données respectueuses des droits des clients.

Un danger demeure néanmoins: même une déclaration de traitement de données ne permet pas d'exclure les abus. C'est le cas si elle ne reflète pas les traitements réellement effectués. Les utilisateurs de services en ligne seront alors induits en erreur.
Nous avons donc rappelé au secrétariat du groupe de travail la nécessité de mentionner clairement sur la page Internet de l'OCDE que le générateur ne peut pas générer automatiquement des déclarations de traitement de données conformes à la protection des données. L'utilisation du générateur peut néanmoins indiquer si, dans le cas d'espèce, la protection des données pratiquée répond aux directives de l'OCDE.
Le générateur de l'OCDE peut être obtenu à l'adresse suivante : http://www.oecd.org/scripts/PW/PWHome.ASP.
Il convient par ailleurs de se reporter aux indications en vue de l'établissement d'une déclaration de traitement des données sur Internet (voir page 158).

- Signatures digitales

Conformément à la déclaration adoptée par les ministres à l'issue de la Conférence d'Ottawa de 1998 sur l'authentification électronique, le comité de l'ICCP a chargé un comité ad hoc de rédiger un rapport sur la situation en la matière. Ce rapport devra présenter les voies et moyens par lesquels l'authentification électronique pourra progresser. Il analysera aussi les réglementations nationales qui existent déjà à ce propos.

La signature digitale jouant aussi un rôle important dans la protection de la sphère privée, nous avons proposé d'examiner la question de la compatibilité des différents modèles nationaux.
Dans de nombreux pays, il existe déjà sur le sujet des lois ou des projets de loi dont l'entrée en vigueur est prochaine. Il convient à cet endroit de mentionner que dans tous les pays de la Communauté européenne sans exception, les lois

sur la signature digitale sont conformes à la directive européenne récemment adoptée à ce propos
(cf. http://www.europa.eu.int/comm/dg15/en/media/sign/99-915.htm).
Compte tenu de l'évolution de la question au niveau européen et de la nécessité de disposer de systèmes compatibles, nous estimons dans l'intérêt de la Suisse de veiller à l'eurocompatibilité de son projet de loi sur la signature digitale.

- Forum sur le commerce électronique

Les 12 et 13 octobre 1999, Paris a accueilli un forum sur le commerce électronique. Organisé dans le sillage de la Conférence d'Ottawa sur le commerce électronique, il avait pour objet de contrôler l'application des déclarations ministérielles adoptées à l'issue de cette conférence et d'examiner la marge de manœuvre de l'OCDE dans ce domaine.

Bien que les nouvelles technologies aient un impact stimulant sur l'économie, le commerce électronique n'inspire pas encore vraiment confiance aux utilisateurs. Les organisations internationales, les Etats et les particuliers doivent mettre en place des conditions-cadres incitant l'utilisateur à se sentir davantage en confiance et en sécurité. Le commerce électronique ne se développera que si le consommateur a effectivement les moyens de protéger sa sphère privée. Auto-régulation du marché ou codes de conduite ne pourront résoudre à eux seuls les différents problèmes posés. Il convient donc de viser un équilibre entre codes de conduite et réglementations étatiques.

Dans la mesure où les codes de conduite ne peuvent assurer une protection efficace de la sphère privée, nous estimons qu'il faut impérativement établir des réglementations étatiques.

5. Projet d'Accord franco-suisse de coopération transfrontalière

Dans le cadre du « groupe de travail France », nous avons participé à l'élaboration du projet d'Accord franco-suisse relatif à la coopération transfrontalière en matière judiciaire, policière et douanière. Des dispositions spécifiques de protection des données ont été élaborées afin de régler les traitements de données personnelles qui seront effectués dans le cadre de cet Accord. Ce dernier prévoyant en outre la mise en service de centres communs installés à proximité de la frontière, nous avons rendu attentif le groupe de travail sur la nécessité de déterminer quels systèmes informatiques y seront

installés en regard des bases légales existantes et des dispositions réglant les accès à ces systèmes.

Le 20 avril 1999 l'Assemblée fédérale a ratifié l'Accord franco-suisse du 11 mai 1998 relatif à la coopération transfrontalière en matière judiciaire, policière et douanière. Du côté suisse, les conditions requises pour l'entrée en vigueur ont ainsi été remplies. Le gouvernement français a quant à lui déposé en automne 1999 un projet de loi d'approbation devant le Parlement en vue de son traitement par le Sénat et son approbation par l'Assemblée nationale. En l'absence de difficultés au cours de la procédure française, l'entrée en vigueur de cet Accord pourrait avoir lieu d'ici l'automne 2000.

Invités à participer à l'élaboration de cet Accord dans le cadre du « groupe de travail France » placé sous la conduite de l'Office fédéral de la police et de l'Office fédéral des étrangers, nous avons mis en évidence la nécessité d'y prévoir des dispositions spécifiques de protection des données. Ces dispositions ont fait l'objet d'un examen attentif tant au sein du « groupe de travail France » que par les négociateurs français. Ces travaux ont permis l'élaboration d'une norme détaillée de protection des données réglant les traitements de données personnelles qui seront effectués dans le cadre de cet Accord. Cette norme rappelle en effet les principes généraux applicables en la matière, règle les conditions de collecte, de communication et de conservation des données et prévoit la mise en place de mesures techniques et organisationnelles appropriées pour protéger les données contre tout accès ou traitement non autorisé.

Dans le cadre de la mise en application de cet Accord, il est prévu la mise en service de centres de coopérations communs aux deux parties qui seront installés à proximité de la frontière. Le « groupe de travail France » s'est prononcé en faveur de l'implantation d'un premier centre commun à l'aéroport de Genève. En complément à l'examen des coûts liés à l'installation et à l'exploitation de ce centre commun, nous avons rendu attentif le groupe de travail à la nécessité d'examiner également concrètement quels systèmes informatiques seront utilisés pour les traitements de données et quels sont les accès qui sont envisagés. Le groupe de travail, relevant la pertinence de cette mise en garde, a donné mandat au représentant de l'Office fédéral de la police d'examiner quelles sont les banques de données fédérales et cantonales qui seraient concernées dans le cadre de ces centres communs et de dresser un inventaire des lois ou ordonnances applicables ainsi qu'une liste des éventuelles normes qui devraient le cas échéant être révisées.

6. Groupe de travail international pour la protection des données dans le domaine des télécommunications

Le 31 août 1999, l'occasion nous a été donnée de prendre part à la 26e séance à Berlin du groupe de travail auquel nous participons régulièrement. Outre l'information des participants sur les derniers développements touchant à la protection des données qui ont eu lieu dans le domaine du droit des télécommunications des divers pays, l'accent fut mis sur les problèmes de protection des données dans l'Internet.

Lors d'un symposium public organisé dans le cadre du salon « Internationale Funkausstellung » de Berlin sur le thème « Protection des données – un pont entre la vie privée et le marché mondial » par le délégué à la protection des données berlinois, nous avons entre autres discuté des moyens à mettre en œuvre pour continuer à défendre les droits de la personnalité des consommateurs face à la mondialisation croissante des marchés (thème du commerce électronique). D'autre part, nous avons pu assister à la présentation de possibilités technologiques respectueuses de la protection des données. Une documentation détaillée du symposium peut être consultée à l'adresse http://www.datenschutz-berlin.de/infomat/heft27/index.htm.

IV. PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES

1. Sixième Conférence suisse des Commissaires à la protection des données

La sixième Conférence des Commissaires à la protection des données, organisée par le PFPD, s'est tenue le 5 novembre 1999 à Berne. Des représentants des autorités cantonales de protection des données ainsi que des conseillers à la protection des données des départements fédéraux ont participé à cette conférence. Le thème principal fut celui du principe de la transparence qui exige que des dossiers administratifs doivent par principe être rendus accessibles au grand public. L'objectif est de promouvoir le débat démocratique ainsi que le contrôle de l'activité de l'Etat. Les expériences de la loi sur l'information du canton de Berne, qui est déjà en vigueur depuis plusieurs années, le projet de loi fédérale ainsi que le projet de loi du canton de Soleure ont été présentés. D'autre part, une étude comparée des législations étrangères relatives à ce thème a été exposée. Le thème central fut la question de savoir comment il était possible d'offrir la transparence tout en préservant la protection des données

personnelles. Vous trouverez un article sur le thème principe de la transparence et protection des données à la page 203 de ce rapport.
Parmi les autres thèmes traités, on peut citer les prestations de service électroniques des administrations cantonales (e-government), le recensement fédéral 2000 ainsi que les banques de profils d'ADN utilisées à des fins d'identification judiciaire.

2. Les publications du PFPD - Nouvelles parutions

- Aide-mémoire «SPAM: Qu'est-ce et comment s'en protéger»
- Aide-mémoire relatif à la protection des données lors de l'utilisation du téléphone au lieu de travail
- Aide-mémoire concernant le traitement d'adresses de membres d'une association

Vous trouverez tous les aide-mémoire en annexe du présent rapport (voir page 238). Ils peuvent également être consultées sur notre site Web (www.edsb.ch).

- Feuille d'information du PFPD 2/1999
- Feuille d'information du PFPD 1/2000

Les feuilles d'information peuvent être consultées sur notre site Web (www.edsb.ch).

3. Statistique des activités du Préposé fédéral à la protection des données Période du 1er avril 1999 au 31 mars 2000

Participations à des conférences

Nationales	Internationales
18	17

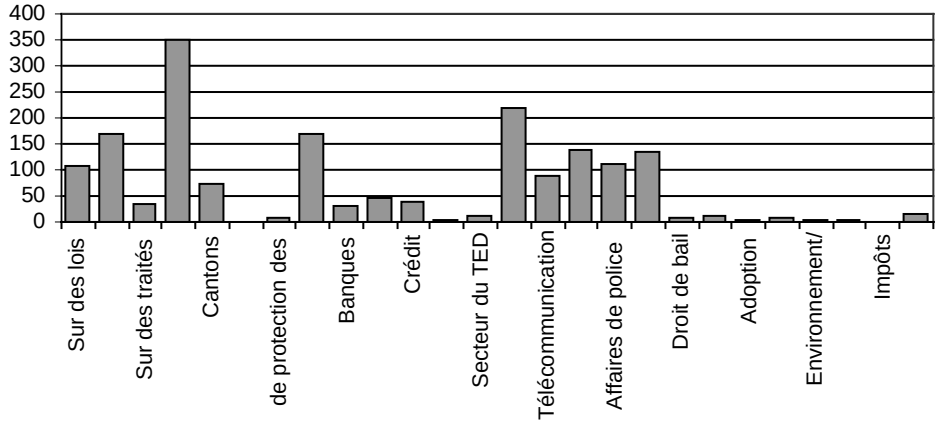
Nombre de séances

	Confédération	Personnes privées	Cantons
A l'intérieur	189	66	9
A l'extérieur	258	49	21
Total	447	115	30

Nombre de prises de position

	Entrées	Prises de position écrites	Recommandations du PFPD	Pas d'objections
Sur des lois	51	53		3
Sur des ordonnances	80	74		15
Sur des traités internationaux	16	14		4
Questions du secteur public:				
Organes fédéraux	182	164	2	1
Cantons	40	35		
Autorités étrangères de protection des données	4	4		
Questions du secteur privé:				
Personnes privées	90	79		
Banques	19	13		
Vente d'adresses / Marketing direct	24	24		
Crédit	23	14		
Librairies/Publications	2	2		
Secteur du TED	5	5		
Personnel	121	98	1	
Télécommunication	44	44	2	
Assurances	83	54		
Affaires de police	53	58		
Santé	75	60		
Droit de bail	4	4		
Carte client	6	6		
Adoption	1	1		
Sectes	3	3		
Environnement / constructions	1	1		
Associations	2	2		
Impôts	1			
Douanes	8	4		4
Total	938	816	5	27

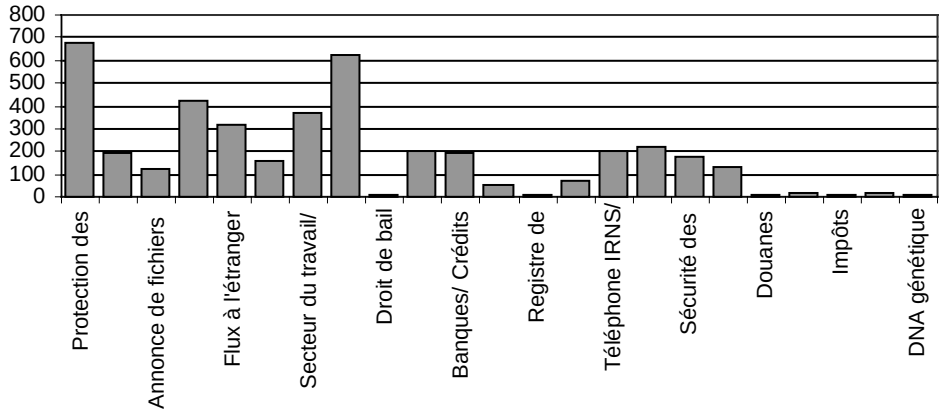
Nombre de prises de position



RENSEIGNEMENTS PAR TELEPHONE

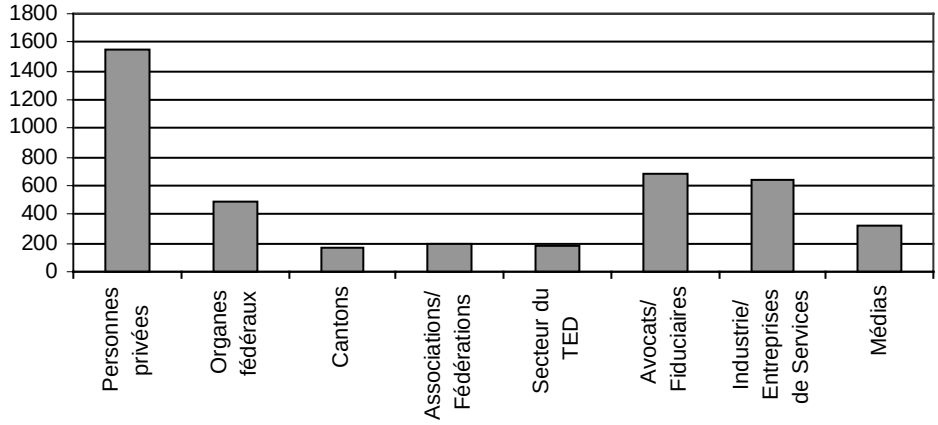
Renseignements par téléphone

par matière



Renseignements par téléphone

selon la provenance des appels



4. 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 :	Atia-Off Katrin, dr en droit Costa Giordano, lic. en droit Horschik Matthias, Fürsprecher Jakob-Wiederkehr Rita, Fürsprecherin Kardosch Milica, lic. en droit Schönbett Frédéric, lic. en droit Tsiraktsopulos Kosmas, lic. en droit
Service informatique :	Baumann Pierre-Yves, lic. ès sc. math., informaticien Scherrer Urs, informaticien Stüssi Philipp, lic. sc. nat., informaticien
Chancellerie :	Blattmann Doris Purro Isabelle

V. ANNEXES

1. SPAM : Qu'est-ce et comment s'en protéger

Le Préposé fédéral à la protection des données informe :

SPAM : Qu'est-ce et comment s'en protéger

SPAM, c'est quoi ??

La poste électronique est rapide, d'un emploi aisé, et peu coûteuse. Elle permet d'envoyer des messages vers n'importe quel point de la planète en quelques secondes, et ceux qui recourent à ce moyen de communication sont toujours plus nombreux. Les annonceurs n'ont évidemment pas tardé à reconnaître les avantages de cette technologie et ils l'utilisent de plus en plus pour diffuser leurs messages publicitaires. Et c'est ainsi qu'est apparu le "spam", qui, dans le jargon du métier, désigne les envois en masse par courrier électronique. Ce procédé, aussi appelé "junk mail" ou "unsolicited bulk e-mail" irrite fortement les destinataires car il peut aller jusqu'à les perturber dans leur travail, tout en surchargeant le réseau, parfois au point de bloquer toute communication. Pour corser le tout, les destinataires peuvent subir des frais de communication plus élevés.
La présente notice a pour but de vous donner un aperçu des moyens techniques auxquels vous pouvez recourir pour vous protéger et indique les voies de droit offertes par la loi sur la protection des données.

Comment on s'empare de votre adresse e-mail

Chaque fois que vous utilisez l'internet, vous laissez des traces de votre passage, le plus souvent à votre insu, mais aussi volontairement, par exemple lorsque vous fournissez votre adresse électronique et d'autres données personnelles en participant à des groupes de discussion et des sites de causerie, en vous abonnant à des listes de diffusion, en passant des commandes, ou simplement en visitant des sites. Au moyen de logiciels spéciaux, il est possible de scanner des pages internet et des répertoires pour y relever les adresses de courrier électronique et établir des listes de publipostage.

./.

Moyens techniques de protection

Mesure	Exemple	Avantage	Inconvénient
Blocage de votre adresse au moyen d'une liste de blocage	www.erobinson.com/html/eintragung.html	Ne nécessite pas de configuration spéciale auprès du fournisseur ou de l'utilisateur.	Les "Spammers" ne prennent pas tous la peine de vérifier ces listes; il faut donc compter sur leur bonne volonté. Une telle liste peut même être utilisée à des fins publicitaires.
Filtrage du courrier selon certains critères dans l'en-tête ou le corps du texte (mots clés).	Auprès du fournisseur d'accès à Internet ou du site de messagerie	Les paramètres de filtrage peuvent être régulièrement adaptés	On risque aussi de filtrer d'authentiques messages personnels
Bloquer certaines adresses	Procédé possible avec la plupart des logiciels et services de messagerie.	L'expéditeur dont l'adresse est bloquée ne peut plus vous adresser de messages.	Les "spammers" peuvent changer fréquemment d'adresses d'expéditeur, voire recourir à des adresses fictives.
Etablir une liste positive	www.coldmail.de	Ne garanti pas l'élimination des messages indésirables	L'envoi d'un premier courrier reste toujours possible
Utiliser plusieurs comptes de courrier électronique		Il est toujours possible de protéger un compte de messagerie en ne fournissant son adresse que de manière très restrictive	Complique le travail de l'utilisateur
Éviter d'indiquer son adresse électronique (groupes de discussion, listes de diffusion, commandes, sites)			Le destinataire ne peut être atteint que difficilement. Certains services ne sont pas utilisables sans qu'on indique son adresse électronique.
Fournir une adresse électronique modifiée	Laisser un espace avant et après le signe @		Pas toujours reconnu comme adresse électronique par le serveur

Que faire si vous êtes déjà victime de "spamming" ?

Essayez d'identifier le "spammer" en examinant les rubriques de l'en-tête (voir par exemple : http://www.rhein-neckar.de/~ancalago/faq/headrfaq.html)
Intervenez auprès de l'expéditeur et au fournisseur de service par lequel transite le courrier que vous voulez bloquer. Le fournisseur de service peut prendre des mesures appropriées.

Que peut-on entreprendre contre le "spamming" sur le plan juridique ?

Quand vous avez identifié l'adresse du "spammer", faites-lui savoir que vous ne souhaitez pas qu'il vous adresse des messages publicitaires. Demandez-lui de supprimer votre adresse de ses listes de diffusion (verrouillage de l'adresse).

En outre, en vertu de **l'article 8 de la loi sur la protection des données**, vous avez le droit d'exiger du détenteur d'une liste qu'il vous indique quelles données vous concernant sont en sa possession.

Le lésé peut faire valoir ses droits par voie judiciaire (art. 15 LPD)
(voir à ce sujet le guide du PFPD sur les droits relatifs à la protection des données personnelles)

ATTENTION :

La législation suisse sur la protection des données ne s'applique qu'aux personnes qui traitent des données en Suisse. Vous devez donc faire attention où vous inscrivez votre adresse. Si l'usage abusif de votre adresse électronique est commis en dehors de Suisse, le recours aux voies de droit devient extrêmement difficile. Dans de tels cas, la législation en vigueur dans le pays où est traitée l'adresse électronique, est applicable.

Pour plus d'informations sur ce thème, vous pouvez consulter par exemple les sites suivants :

http://www.politik-digital.de/spam/de/links/
http://www.imc.org/imc-spam
http://www.spam.abuse.net/
http://www.pobox.com/~djb/qmail.html
http://www.sendmail.org/antispam.html

Vous pouvez trouver d'autres adresses internet en faisant une recherche au moyen du mot clé **"antispam" .**

La présente notice et d'autres informations sur ce thème peuvent aussi être consultées sur notre site http://www.edsb.ch .

2. Aide-mémoire relatif à la protection des données lors de l'utilisation du téléphone au lieu de travail

Le groupe de travail des préposés des cantons et du préposé fédéral à la protection des données informent :	Aide-mémoire relatif à la protection des données lors de l'utilisation du téléphone au lieu de travail (pour les administrations publiques et les entreprises privées)

La sphère privée du travailleur est protégée à son lieu de travail. L'employeur est tenu, en vertu du Code des obligations[1], de prendre les dispositions nécessaires pour garantir la protection de la personnalité du travailleur. De son côté, le travailleur doit exécuter avec soin le travail qui lui est confié et sauvegarder fidèlement les intérêts légitimes de l'employeur[2] (éviter l'abus du téléphone pour des motifs privés, les risques pour la sécurité, par exemple). L'usage de systèmes de surveillance pour contrôler le respect des intérêts de l'employeur ou à des fins de sécurité peut représenter une atteinte inadmissible à la sphère privée du travailleur si certaines conditions ne sont pas observées[3]. Le travailleur lésé peut faire valoir des prétentions de droit civil en cas d'atteinte à sa personnalité; il peut en outre déposer une plainte pénale[4].

A. Usage privé du téléphone au lieu de travail

En l'absence de restriction expresse ou d'interdiction des appels privés au lieu de travail, le travailleur peut partir du principe que l'usage privé du téléphone est autorisé dans des limites raisonnables et qu'aucune surveillance n'est effectuée.

1. Interdiction des écoutes et de l'enregistrement des conversations privées

La surveillance des conversations téléphoniques privées par l'employeur, que ce soit sous forme d'écoute ou d'enregistrement des conversations, constitue une surveillance du comportement et fait l'objet d'une interdiction. Cette règle s'applique aussi bien en l'absence de réglementation de l'usage du téléphone au lieu de travail qu'en cas de restriction expresse ou d'interdiction des appels téléphoniques privés au lieu de travail. En cas d'interdiction expresse des appels privés au moyen du téléphone professionnel, le travailleur doit pouvoir disposer d'un appareil téléphonique non surveillé et permettant le paiement au moyen de pièces de monnaie ou d'une carte de paiement.

2. ***Enregistrement de données relatives aux appels privés à des fins de facturation***

Les données relatives aux appels téléphoniques[5] relèvent de la sphère privée et ne doivent en principe pas être saisies. Toutefois, l'indicatif peut être enregistré. Un extrait détaillé des taxes (avec les numéros complets) des appels téléphoniques privés n'est établi que sur demande expresse ou avec l'accord de l'intéressé[6]. Dans ce cas, le traitement doit viser uniquement la vérification mutuelle des taxes facturées. Les numéros appelés à des fins d'entretiens privés ne

---

[1] Art. 328 du Code des obligations (CO, RS 220). Confédération et cantons peuvent édicter leurs propres dispositions.

[2] Art. 321a CO

[3] Art. 26 de l'ordonnance 3 relative à la loi sur le travail (RS 822.113)

[4] Art. 179bis du Code pénal (CP, RS 311.0)

[5] Eléments d'adressage (numéros de téléphone), l'heure des communications, la rémunération due

[6] Art. 13 Abs. 1 de la loi sur la protection des données (LPD, RS 235.1)

doivent pas être communiqués à des tiers (par exemple aux supérieurs hiérarchiques). Les données ainsi saisies doivent être détruites au plus tard après le paiement des taxes facturées.

Il est souhaitable que le travailleur ait la possibilité de décider, par un moyen simple, par exemple en appuyant sur une touche avant l'appel, si la conversation téléphonique est de nature privée ou professionnelle. Un tel moyen permet de réduire le risque qu'un entretien privé ou même simplement le numéro privé appelé soit enregistré. La loi sur les télécommunications[7] autorise l'employeur à demander au fournisseur de services de télécommunication des paramètres d'adressage identifiables dans sa facturation. En pratique, il est fréquent que le fournisseur communique ces éléments spontanément. Il est recommandé de régler cette question avec le fournisseur et d'en parler avec le travailleur; il convient aussi d'en faire mention dans les directives internes de l'administration ou de l'entreprise concernant l'usage du téléphone au lieu de travail.

3. ***Enregistrement des données relatives aux appels privés dans le but d'empêcher l'abus du téléphone à des fins privées***

Par abus du téléphone à des fins privées ont entend aussi bien l'inobservation d'une restriction ou d'une interdiction de l'usage privé du téléphone qu'une utilisation disproportionnée du téléphone pour des motifs privés. La surveillance d'un tel abus doit se fonder sur des indices qui ne découlent pas d'un contrôle préventif des données relatives aux appels. Tel est en particulier le cas lorsque les données ne sont pas anonymisées. Les indices d'une suspicion légitime peuvent consister par exemple en un montant exagérément élevé des taxes téléphoniques d'un collaborateur, une baisse marquée de ses performances, ou l'observation répétée d'un abus. Après avoir constaté de tels indices, il y a lieu d'en informer le travailleur concerné, en lui faisant savoir que des enregistrements et des évaluations des données relatives aux appels pourront être effectués (pour ce qui est d'une utilisation du téléphone pour la commission d'un délit, voir le point C, page 4). A cette occasion, on accordera au collaborateur la possibilité de fournir une justification. L'employeur est tenu, dans un tel cas, de garder confidentielles les données relatives aux appels privés ainsi obtenues. La constitution d'un délit d'écoute de conversations de tiers est en tous les cas réservée.

Par contre, si l'utilisation du téléphone à des fins privées est expressément interdite, des contrôles des données d'adressage complètes ne sont admises de la part de l'employeur que s'ils ne se font pas de manière systématique, mais seulement par sondage au hasard et que sur requête du chef. En outre, il faut que les employés aient été préalablement informés de la possibilité de ces contrôles.

Récapitulation

- *Les appels téléphoniques privés au lieu de travail sont en principe autorisés, pour autant que la proportionnalité soit respectée et qu'aucune restriction ou interdiction expresse de l'employeur n'ait été prononcée.*
- *La mise sous écoute ou l'enregistrement de la teneur des appels téléphoniques privés sont absolument interdits.*
- *L'enregistrement et l'examen des données complètes relatives aux appels téléphoniques privés sont en principe interdits.*

Exceptions

- facturation au collaborateur à sa demande expresse;

[7] Art. 45 Abs. 1 de la loi sur les télécommunications (LFT, RS 784.10)

- *Cas où l'utilisation du téléphone à des fins privées est en principe admise, mais disproportionnée : constatation de l'abus sur la base d'indices extérieurs et à condition que la personne concernée soit informée que l'enregistrement et l'examen des données complètes relatives aux appels sont possibles dès la constatation d'abus.*
- *Cas où l'utilisation du téléphone à des fins privées est expressément interdite : contrôle des données d'adressage complètes des appels privés, pour autant qu'on ne procède pas systématiquement, mais par sondage et sur ordre du supérieur hiérarchique, pour autant que les employés ont été expressément informés de la possibilité de tels contrôles.*

- *Le délit d'écoute ou d'enregistrement des appels téléphoniques de tiers est dans tous les cas réservé.*
- *Il est conseillé d'édicter des directives internes aux administrations et entreprises sur l'utilisation du téléphone au lieu de travail.*

B. Appels téléphoniques professionnels au lieu de travail

1. Écoute ou enregistrement d'entretiens téléphoniques professionnels

S'il est expressément interdit au collaborateur d'effectuer des appels privés au moyen de son téléphone professionnel, ou s'il est techniquement ou pratiquement impossible de distinguer efficacement entre appels privés et professionnels, il est admissible de procéder à une écoute ou un enregistrement des appels professionnels, pour autant que cela soit absolument nécessaire pour des motifs d'exploitation (contrôle de performance ou de sécurité). Il faut en outre faire en sorte que le collaborateur concerné et son interlocuteur soient clairement informés à l'avance (par exemple au moyen d'un signal acoustique ou optique) chaque fois que leur entretien téléphonique sera mis sur écoute. La constitution d'un délit en cas d'écoute ou d'enregistrement de conversations avec des tiers sans l'accord des personnes concernées est réservée. L'écoute ou l'enregistrement pour motifs de sécurité est cependant admissible lorsqu'ils sont nécessaires à des fins d'obtention de preuves (par exemple l'enregistrement d'entretiens portant sur des affaires juridiques traitées par téléphone). La surveillance du comportement est interdite, même pour les appels téléphoniques professionnels.

Il y a contrôle de la performance lorsque l'écoute ou l'enregistrement sont destinés à servir à des fins didactiques. La surveillance du comportement n'est par contre pas autorisée (art. 26 de l'ordonnance 3 relative à la loi sur le travail).

Lorsqu'il n'est techniquement ou pratiquement pas possible de distinguer entre appels professionnels et privés, il est possible d'éviter l'écoute ou l'enregistrement d'appels privés dans le cadre d'un contrôle de performance ou de sécurité portant sur les communications téléphoniques professionnelles en informant à l'avance les collaborateurs et interlocuteurs concernés de la durée précise de la période de contrôle, qui doit se limiter au strict minimum nécessaire.

2. Enregistrement de données relatives aux appels professionnels

Les installations téléphoniques actuelles permettent d'enregistrer par des procédés simples des données relatives aux communications téléphoniques d'un collaborateur. Les données concernant les appels professionnels ne peuvent être enregistrées que lorsque ceci est nécessaire pour des motifs administratifs (par exemple pour assurer la transparence des frais de téléphone ou pour permettre la facturation aux clients) et pour autant qu'aucun contrôle du comportement ne soit effectué. Le transparence des frais de téléphone d'une organisation est de toute manière assurée même si on ne connaît pas en détail quel collaborateur a téléphoné

sur un raccordement donné et pour combien de temps. Il suffit de savoir à combien se montent les frais de téléphone pendant une période déterminée.

Récapitulation

- *Les appels téléphoniques professionnels ne peuvent être mis sur écoute ou enregistrés qu'à des fins de contrôle de performance ou de sécurité et seulement après que les interlocuteurs concernés en ont été dûment informés*
- *Tout appel faisant l'objet d'une écoute ou d'un enregistrement doit être signalé au moyen d'un procédé acoustique ou optique.*
- *La constitution d'un délit d'écoute ou d'enregistrement d'entretiens de tiers est réservée.*
- *Il est recommandé d'établir des normes claires concernant les contrôle de performance ou de sécurité dans les directives internes des administrations et des entreprises relatives à l'utilisation du téléphone au lieu de travail.*

C. Cas particulier de l'utilisation du téléphone pour commettre un acte délictueux

Lorsqu'on soupçonne l'existence d'un comportement illicite, c'est-à-dire non seulement contraire au contrat de travail (et le cas échéant à la directive concernant l'utilisation du téléphone au lieu de travail), la protection de la sphère privée doit nécessairement passer au second plan. Si un collaborateur est soupçonné d'escroquerie, d'atteinte à l'honneur de l'employeur ou d'autres délits, l'autorité pénale est habilitée à effectuer ou à ordonner, à la demande de l'employeur, sans en informer préalablement la personne concernée et dans les limites fixées par les dispositions légales applicables en matière de surveillance des télécommunications, des écoutes ou des enregistrements téléphoniques aux fins d'obtention de preuves. Ceci est valable tant pour les appels privés que professionnels. Une telle surveillance ne constitue pas un contrôle de performance ou de sécurité. Elle se justifie lorsque, après pondération des intérêts en jeu par l'autorité pénale, il existe un intérêt public ou privé prépondérant en ce sens. Les données ainsi obtenues doivent être traitées confidentiellement et détruites dès que le but de l'enregistrement est atteint. L'employeur n'a en aucun cas le droit de prendre des mesures d'obtention de la preuve sans faire intervenir l'autorité judiciaire compétente. De telles mesures représenteraient non seulement une violation de la sphère privée du collaborateur mais pourraient être considérées comme des moyens illicites d'obtention de preuves dans le cadre d'une procédure judiciaire. Des surveillances et des enregistrements d'appels sans l'intervention de l'autorité compétente peuvent exceptionnellement être exécutées par l'employeur, s'il existe un danger concret de perte de la preuve. L'employeur reste cependant tenu d'en informer l'autorité compétente dès que possible.

Récapitulation
Lorsque l'employeur recourt à une écoute ou un enregistrement téléphonique à des fins d'obtention de preuves, il doit faire intervenir l'autorité pénale compétente, à moins qu'il existe un danger concret de perte de la preuve. Dans ce dernier cas, l'employeur reste tenu d'informer les autorités compétentes dès que possible.

D. Caractéristiques particulières des installations téléphoniques

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

1. Appareils "mains libres" munis d'un haut parleur

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

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

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

2. Affichage du numéro de l'appelant

Avant même le commencement d'une conversation téléphonique, le numéro de l'appelant s'affiche (le cas échéant aussi ses nom et prénom).

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

- ➔ L'appelant doit disposer de la possibilité de supprimer l'affichage de son numéro de cas en cas.

3. Liste des appelants

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

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

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

4. Annonce directe ou par haut-parleur

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

Problème: outre le fait que ce procédé dérange les collègues, il permet également une écoute lorsqu'on ne s'aperçoit pas que l'appareil est enclenché.

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

5. Conférence téléphonique

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

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

- ➔ Chaque fois qu'un interlocuteur est connecté ou déconnecté, cela doit être signalé (de manière différenciée) à tous les participants.
- ➔ Il est souhaitable que chaque interlocuteur puisse déterminer le nombre de participants et leur identité.

6. Touches dédiées / voyants

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

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

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

E. Sécurité des données et droit d'accès

L'employeur est tenu de protéger, par des mesures techniques et organisationnelles appropriées, les données personnelles relatives aux liaisons téléphoniques contre toute intervention non autorisée[8]. Il doit en particulier veiller à assurer la confidentialité, la disponibilité et l'intégrité de ces données[9]. Le travailleur peut en tout temps demander à l'employeur si des données le concernant font l'objet d'un traitement[10].

Si vous avez des questions, veuillez vous adresser au Préposé fédéral à la protection des données, 3003 Berne, tél. 031 322 43 95, ou au préposé à la protection des données de votre canton.

[8] Art. 7 Abs. 1 LPD

[9] Art. 8 Abs. 1 de l'ordonnance relative à la LPD (OPD, RS 235.11)

[10] Art. 8 Abs. 1 LPD.

3. Aide-mémoire concernant le traitement d'adresses de membres d'une association

Le Préposé fédéral à la protection des données informe :

AIDE-MÉMOIRE CONCERNANT LE TRAITEMENT D'ADRESSES DE MEMBRES D'UNE ASSOCIATION

Les données personnelles de membres d'une association telles que les adresses doivent être traitées avec soin. L'organe auquel ces données ont été confiées pour l'accomplissement de ses tâches, porte la responsabilité de traiter ces données en accord avec les dispositions de protection des données.
Conformément à la loi fédérale sur la protection des données, des données personnelles ne peuvent être traitées que pour atteindre le but qui a été indiqué lors de leur collecte, qui ressort des circonstances ou qui est prévu par la loi.

Communication à des tiers

La communication d'adresses de membres d'une association à des tiers n'est licite que :

1. si ceci découle clairement des statuts de l'association (formulation aussi précise que possible du but), ou
   Attention : chaque membre a le droit absolu en tout temps de s'opposer à la communication ou de révoquer partiellement ou intégralement un consentement donné précédemment.

2. si le consentement de chaque membre a été préalablement obtenu ou si un droit d'opposition a été consenti à tous les membres après les avoir informé sur le destinataire et sur le but de la communication ou

3. si une obligation légale à le faire existe.

A noter : même une organisation faîtière est considérée dans ce contexte comme une tierce personne. Une association est par principe une personne morale disposant de sa propre personnalité juridique.

Communication à des membres de l'association

La remise de listes des membres à des membres de l'association est autorisée si :

1. la liste est nécessaire pour exercer les droits attachés à la qualité de membre ;
   Exemple : convocation d'une assemblée extraordinaire des membres (art. 64 al. 3 CC).
   Attention : le respect de prescriptions de forme statutaires ne doit pas fortement entraver l'exercice des droits attachés à la qualité de membre.
2. les personnes concernées ont donné leur accord.

A noter : pour prévenir les abus, il est recommandé d'exiger de la part des membres auxquels on remet une telle liste qu'ils fournissent une garantie qu'ils n'utiliseront pas les adresses à d'autres fins, par ex. pour des envois publicitaires.

Droit d'accès // Consultation de la part des membres de l'association de documents les concernant

Selon la loi sur la protection des données, chaque personne ainsi que son représentant légal est en droit de demander à un maître de fichier si des données sont traitées sur sa personne et si oui, lesquelles. Vous trouverez plus de détails concernant le droit d'accès dans le guide « *Les droits de la personne concernée en matière de traitement de données personnelles* » édité par le PFPD.

Accès à des adresses de membres sur le site Web de l'association

Etant donné que l'Internet présente des dangers d'abus spécialement élevés, une telle publication nécessite le consentement des personnes concernées.
Un consentement est légalement valable si les personnes concernées ont été informées au préalable que leurs données sont accessibles dans le monde entier, y compris depuis des pays n'ayant pas de protection des données équivalente à celle qui est garantie en Suisse. Il y a lieu en outre de les rendre attentifs aux risques d'ordre général tels que les maintes possibilités de couplage des données, le fait qu'il n'existe aucune garantie en matière d'intégrité, d'authenticité et de disponibilité.
Vous pouvez obtenir un modèle d'une telle *clause de consentement* auprès du Préposé fédéral à la protection des données.

Prétentions et procédure

En cas de violation des droits de la personnalité, la personne concernée a la possibilité – selon l'art. 15 LPD – de s'adresser à un tribunal civil. Le demandeur peut en particulier requérir que les données personnelles soient rectifiées ou détruites ou que leur communication à des tiers soit interdite. Dans les cas où des droits attachés à la qualité de membre sont violés, il est en outre possible – selon l'art. 75 CC – de s'adresser à un tribunal.

Pour obtenir de plus amples informations sur la protection des données, visitez le site Web www.edsb.ch ou adressez-vous directement au Préposé fédéral à la protection des données, 3003 Berne, Tél. 031/322 43 95.

4. Recommandation du Conseil de l’Europe relative à la protection des données à caractère personnel collectées et traitées à des fins statistiques

Voir version française dans le 5ème rapport d'activités 1997/98 à la page 257.