Préposé fédéral à la protection des données

Rapport d'activités 1998/99

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 1998 au 31 mars 1999.

TABLE DES MATIÈRES

* : Version originale en allemand

* :Version originale en allemand

* :Version originale en allemand

* :Version originale en allemand

AVANT PROPOS

La protection des données à des fins d'intérêt public

En protégeant les données personnelles des individus, une loi sert non seulement un intérêt étatique, mais également un intérêt public. La protection des données se veut en effet au service de l'intérêt général et non pas opposée à cet intérêt. Des tensions sont néanmoins inévitables, notamment lorsque la protection des données s'oppose à un autre intérêt général de caractère équivalent. Nous devons résoudre ce conflit par une mise en balance appropriée des différents intérêts en présence (respect du principe de proportionnalité).
Voir dans la protection des données un frein est dès lors déplacé. A l'inverse, le monde politique, administratif et économique doit concevoir la protection des données comme un objectif. Sa réalisation nécessite des moyens financiers et doit être intégrée dans le développement de systèmes. Ainsi, lors du développement et de la réalisation d'un système de traitement de données, il faut évaluer les conséquences négatives qui peuvent en résulter pour la vie privée.
En tant que personne concernée et consommateur, l'individu doit également réclamer la protection de ses données comme objectif si l'on ne veut pas que cet appel de la protection des données demeure lettre morte. Il doit ainsi être orienté sur les risques inhérents au développement des nouvelles technologies.

Le potentiel des technologies de l'information – un défi pour la protection des données

Grâce au courrier électronique, quelques secondes suffisent aujourd'hui pour adresser ou recevoir, depuis son lieu de travail ou son domicile, des informations à destination ou en provenance de n'importe quel point du globe. Le passage à la société de l'information, annoncé par les milieux spécialisés, se réalise à un rythme tel qu'il devient très difficile de le suivre. Dans tous les domaines, ce développement est caractérisé par un recours intense aux technologies de l'information, lesquelles engendrent un phénomène de dépendance et créent une plus grande exposition aux risques. Les limites temporelles et spatiales des systèmes traditionnels de traitement des données tombent. Des ressources infinies en informations sont ainsi à disposition des individus, des autorités et des entreprises.
Ce développement est un redoutable défi pour la protection de la vie privée. Face aux énormes possibilités offertes par la technologie, la tentation est grande de les utiliser au point de remettre en cause les barrières factuelles qui garantissaient jusqu'à présent les droits des personnes concernées. Des systèmes d'informations en réseau permettent d'avoir accès en ligne sans limites à une

plus grande masse de données et de fichiers, de procéder à leurs comparaisons et de dresser des profils. Il parait dès lors normal que la demande se fasse toujours plus pressante pour recourir à ces instruments au prétexte d'optimiser le potentiel de rationalisation, d'accélérer les procédures administratives et d'offrir un plus grand confort d'utilisation. La réalisation de ces objectifs comporte cependant d'énormes risques.
Ma tâche ne consiste pas pour autant à freiner les développements positifs des technologies de l'information. Au contraire, le recours à ces technologies doit être encouragé. Il faut toutefois en fixer les limites.

Les limites mises au traitement traditionnel des données tombent

Le multimédia et la mise en réseau soulèvent de nouveaux problèmes de protection des données. L'offre de services en ligne n'apporte pas que des avantages et un meilleur confort d'utilisation. Elle permet un impressionnant traçage de données (par ex. l'information sur l'utilisateur d'un service donné, le moment et la durée de l'utilisation). A partir d'informations les concernant, il est ainsi possible de dresser un profil complet des habitudes de consommation de ces individus. Ces profils peuvent aussi intéresser notamment le marché de la publicité, le commerce d'adresses ou l'employeur. Le respect de la vie privée et la sécurité des communications de données s'exposent ainsi à de nouveaux risques. Pour protéger la vie privée, nous estimons indispensable de limiter clairement le traitement aux seules données nécessaires à l'accomplissement d'une tâche déterminée et de fournir des garanties fondées pour le respect des finalités du traitement. Cet objectif ne peut être atteint que si nous complétons le cadre juridique par un recours plus marqué à des solutions techniques.

Dans la société moderne de l'information, les traitements de données ne connaissent pas de limites

Le traitement de données personnelles ne se déroule plus à l'intérieur des frontières nationales. Il revêt une dimension universelle. Les risques d'atteinte à la vie privée qui en résultent ne peuvent être maîtrisés qu'à l'échelle mondiale.
Du fait de l'interconnexion internationale des réseaux et de la quasi impossibilité de déterminer sur quel ordinateur se déroule en temps réel le traitement des données personnelles, nous devons définir au plan universel non seulement des standards de communication, mais également des standards de protection des données prévoyant également des mécanismes de contrôle par des organes de protection des données indépendants. En Europe, nous avons déjà effectué des progrès importants pour le respect international de la vie privée. Dans d'autres pays cependant, et notamment aux Etats-Unis d'Amérique, un niveau

de protection des données adéquat ne sera pas ancré de sitôt dans la législation. Dès lors, il devient urgent de recourir à des technologies et à une organisation du traitement permettant une utilisation des informations conforme à la protection des données ou offrant du moins des options appropriées à des conditions acceptables. Une telle technologie conforme à la protection des données serait certainement un bon argument de vente et de marketing.

Le recours à la technologie de la vie privée

Dans tous les domaines, on recourt aux technologies informatiques. Leur pénétration dans nos activités ne cesse de s'élargir. La communication sur des réseaux digitaux et la participation à des services en ligne sur des réseaux nationaux ou internationaux génèrent quantités de données individuelles. A partir de ces traces électroniques, nous pouvons dresser des profils de la personnalité sur le comportement des individus.
Le nombre de personnes recourant à ces technologies ne cesse d'augmenter. Toutefois du fait de la complexité des systèmes d'informations et de leur manque de transparence, l'individu n'est en règle générale pas en mesure de connaître la nature et l'étendue des données collectées le concernant, le lieu et la durée de leur conservation, ainsi que la finalité pour laquelle elles sont traitées. Il n'est également pas armé pour user des possibilités de contrôle qui lui sont offertes.
Lors de l'utilisation de ces systèmes, il est néanmoins possible de garantir aux personnes le respect de leur vie privée, notamment en limitant l'accès aux données par des mesures techniques et organisationnelles. Cette protection repose ainsi essentiellement sur l'efficacité des mesures de sécurité traditionnelles et sur le recours à des technologies de la vie privée. Ainsi, l'augmentation des risques d'atteinte à la vie privée des individus peut efficacement être compensée par une réduction conséquente du nombre des données enregistrées. Les personnes qui recourent à ces nouvelles technologies de communication ne pourront à l'avenir assurer la protection des données que si elles y intègrent des technologies de la vie privée.

Le chiffrement – instrument important de la protection de la vie privée

Parmi les technologies les plus importantes de la vie privée, on trouve différentes formes d'application du chiffrement des données. Il existe ainsi des procédures qui offrent à chaque utilisateur une autoprotection optimale et qui lui permette de déterminer le cercle des personnes ayant accès aux données. Toutefois, les autorités de poursuite pénale et les services de renseignements estiment que ces mécanismes diminuent par trop les possibilités de surveillance

et ils souhaiteraient réglementer le recours aux procédures de chiffrement. A ce sujet, j'ai déjà pris position dans mon dernier rapport (5e rapport d'activités, p. 222). Du point de vue de la protection des données, les technologies de chiffrement ne doivent pas être perçues comme une menace. Au contraire, il s'agit d'un instrument remarquable pour protéger efficacement la vie privée. Le danger pour la société ne vient pas des technologies de chiffrement, mais des réglementations qui veulent en diminuer l'efficacité. L'argument selon lequel la criminalité organisée pourrait se servir de ces technologies n'est pas pertinent. En effet, c'est bien en recourant à des procédure de chiffrement puissant que les individus et l'économie peuvent se préserver des attaques criminelles, notamment lors d'opérations de commerce électronique. L'Etat ne doit pas entraver l'utilisation de ces technologies. Il doit plutôt en encourager le développement et la diffusion afin de prévenir autant que possible les infractions pénales.

La société de l'information de demain – une perspective du futur

Le développement très rapide des technologies de l'information ces dernières années appelle à la prudence lorsqu'il s'agit de faire des prévisions pour le futur. Personne ne peut prédire que sera la société de l'information de demain. La direction prise est néanmoins déjà perceptible. L'interconnexion ira en augmentant. L'échange de données automatisé s'intensifiera. Les individus s'acquitteront ainsi de nombreuses tâches quotidiennes au travers de services en ligne. Une masse de données sera communiquée dans le monde entier de manière électronique.
Les normes sur lesquelles se fondera la société de l'information seront différentes de celles auxquelles les juristes se sont habitués. Elles seront influencées par les forces d'innovation. Dans ce contexte, il ne faut pas oublier que les technologies de l'information et de la communication sont développées par des hommes et utilisées par eux. Si des alternatives existent, ce sont toujours des hommes qui décideront dans quelles directions ces technologies seront appliquées.

Le degré d'acceptation des nouvelles technologies est étroitement lié à la garantie de la protection des données et du respect de la vie privée des individus. On peut ainsi prévoir que dans un proche avenir, les produits et les services conformes aux exigences de la protection des données seront plus concurrentiels que les autres. Le consommateur privilégiera les produits et les services qui nécessitent le traitement de peu de données personnelles au détriment de ceux qui laissent des traces importantes.
Il existe actuellement sur le marché un nombre important de technologies et de moyens auxiliaires permettant d'assurer une meilleure protection des données. Une technologie qui permet d'enregistrer, d'utiliser et de communiquer des

données personnelles, peut également être mise à profit pour garantir le respect de la vie privée des individus. Les technologies modernes de la vie privée «Privacy enhancing technologies (PET)» reposent sur le concept selon lequel il faut éviter de collecter des données personnelles ou du moins il faut se limiter au strict minimum. Elles offrent un système complet de mesures techniques auxquelles il convient de recourir. J'invite les utilisateurs à exiger et encourager le recours à ces technologies dans les systèmes informatiques et le législateur à s'en préoccuper. De même, l'industrie et les fournisseurs de service devraient offrir aux consommateurs des systèmes plus transparents et y intégrer plus systématiquement les technologies de la vie privée. Finalement, la protection des données et les nouvelles technologies ne sont pas opposées. Leurs potentialités doivent cependant être équilibrées afin d'assurer le développement futur de la société de l'information.

Conséquences pour la protection des données

Les modifications de la technologie auront également des conséquences pour la protection des données. Le traitement conventionnel des données sous forme papier touche à sa fin. Nous devons dès lors recourir plus systématiquement aux technologies pour assurer le respect de la vie privée dans la société de l'information, si nous ne voulons pas que la protection des données perde son efficacité. La technologie doit elle-même produire des instruments permettant une protection efficace de la vie privée. Il faut également pouvoir imposer le recours à ces instruments techniques.
La cryptographie est étroitement liée à ces instruments techniques. Ces dernières années, elle s'est développée comme un puissant moyen de protection de la vie privée. Des procédures de chiffrement peuvent contribuer à protéger efficacement l'information contre les risques d'atteinte à la confidentialité et à l'intégrité dans les réseaux.

Le rôle des commissaires à la protection des données à l'avenir

Face aux réseaux ouverts de dimension internationale, l'action des Etats atteint ses limites. Un seul pays n'est plus en mesure de réglementer et contrôler les réseaux globaux. L'Etat ne peut plus protéger de la même manière ses concitoyens qui se meuvent sur ces réseaux. De part la dimension transfrontière de l'interconnexion universelle, les mesures notamment contre la criminalité informatique, restent peu efficaces. Les dispositions nationales de protection des données peuvent être aisément détournées. Tout en ayant à l'esprit leur portée limitée, nous devons dès lors tout mettre en œuvre afin de développer rapidement des standards universels.

Dans l’optique du contrôle de la protection des données, il est important de prendre conscience que l’Etat exercera ses fonctions traditionnelles de protection de manière limitée. Les individus doivent à l’avenir veiller plus intensément à se protéger, notamment en ne communiquant que des données préalablement chiffrées. Le rôle des commissaires à la protection des données doit ainsi s’orienter plus vers le conseil afin d’aider les individus à se protéger contre les risques d’atteinte à leur vie privée. Au côté de leurs tâches traditionnelles de conseil et de contrôle de l’administration et du secteur privé, les commissaires à la protection des données devront, à l’avenir, veiller avant tout à conseiller les individus. Il est incontestable qu’avec la société de l’information, nous aurons encore plus besoin d’une protection des données efficace. La protection des données de demain sera cependant différente de celle des ces dix dernières années. Elle se caractérisera par un recours plus limité à des dispositions juridiques formelles et mettra l’accent plus sur la compétence et le service.

O. Guntern

REPERTOIRE DES ABREVIATIONS

ADN (DNA)	Acide désoxyribonucléique
AELE	Association européenne de libre échange
ASA	Association suisse d'Assurances
AUPER	Système d'enregistrement automatisé des personnes
AVS	Assurance-vieillesse et survivants et invalidité
CAMS	Concordat des assureurs-maladie suisses
CC	Centrale de compensation
CdG-E	Commission de gestion du Conseil des Etats
CEDH	Convention européenne des droits de l'homme
CFPD	Commission fédérale à la protection des données
CP	Code pénal
DFJP	Département fédéral de justice et police
DGD	Direction générale des douanes
DOSIS	Système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants
ETV	Les annuaires électroniques d'usagers
FMH	Fédération des médecins suisses (Foederatio Medicorum Helveticorum)
GEWA	Système de traitement de données en matière de lutte contre le blanchiment d'argent
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
ITC	Informatisation du transit commun
JAAC	Jurisprudence des autorités administratives de la Confédération
LAA	Loi fédérale sur l'assurance-accident
LACI	Loi fédérale sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité
LAI	Loi fédérale sur l'assurance-invalidité
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LBA	Loi fédérale relative à la lutte contre le blanchissage d'argent dans le secteur financier
Leg	Loi fédérale sur l'égalité entre femmes et hommes
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
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi sur la protection des données
Lstup	Loi fédérale du 3 octobre 1951 sur les stupéfiants
NSTI	Nouveau système de Transit Informatisé
OACI	Ordonnance sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité
OAMal	Ordonnance sur l'assurance-maladie
OFAM	Office fédéral de l'assurance militaire
OFAP	Office fédéral des assurances privées
OFAS	Office fédérale des assurances sociales
OFE	Office fédéral des étrangers

OFEFP	Office fédéral de l'environnement, des forêts et du paysage
OFI	Office fédéral de l'informatique
OFP	Office fédéral de police
OFS	Office fédéral de la statistique
Oinv	Ordonnance sur les systèmes d'information et de paiement de l'assurance-chômage
OK	Crime organisé
OM	Loi fédérale sur l'organisation militaire
OPAS	Ordonnance sur les prestations de l'assurance des soins
O-PLASTA	Ordonnance sur le système d'information en matière de placement et de statistique du marché du travail
Oren	Ordonnance sur le renseignement
PA	Loi fédérale sur la procédure administrative
PFPD	Préposé fédéral à la protection des données
PISEDI	Système de gestion du personnel du département fédéral de l'intérieur
RAI	Règlement sur l'assurance-invalidité
RCE	Registre central des étrangers
REG-LBA	Registre de l'Autorité de contrôle en matière de lutte contre le blanchissage d'argent
RIPOL	Système de recherches informatisées de police
RNIS	Réseau numérique à intégration de services
SG DFI	Secrétariat général du département fédéral de l'intérieur
StF	Loi fédérale sur le statut des fonctionnaires
UE	Union européenne
ZAN	Index central des dossiers
ZEK	Centre d'informations de crédits
ZSD	Services des offices centraux

I. THEMES CHOISIS

1. Affaires de police

1.1. Loi fédérale concernant la surveillance du trafic postal et des télécommunications – délibérations dans les Chambres fédérales

Le 27 novembre 1998, la loi fédérale sur la surveillance du trafic postal et des télécommunications a été soumise pour délibération à la Commission juridique du Conseil national. Après avoir entendu plusieurs experts, entre autres le Préposé fédéral à la protection des données, la Commission juridique a décidé de mettre en place une sous-commission chargée d'élaborer un contre-projet à la loi fédérale avec l'appui d'experts.

Suite au rapport de la Commission d'enquête parlementaire concernant le Département fédéral de justice et police (CEP), la Commission de gestion du Conseil national (CdG) a mandaté un groupe de travail de vérifier les pratiques de surveillance de la Confédération. La CdG a consigné les résultats de ce groupe de travail dans un rapport du 9 novembre 1992 adressé au Conseil fédéral. Elle a demandé entre autres que soient créées des dispositions plus strictes pour l'écoute des conversations téléphoniques à des fins de poursuite judiciaire. Avec la motion 93.3205 de la CdG du 24 mai 1993, qui a été entérinée par le Conseil fédéral le 14 juin 1993, les contenus suivant ont été imposés pour les travaux législatifs: création d'un catalogue restrictif des délits (complété par une clause générale), meilleure protection de personnes tierces non impliquées, en particulier de personnes habilitées à refuser de témoigner ainsi qu'un contrôle subséquent de l'efficacité. En octobre 1993, le DFJP a mis sur pied le groupe d'étude «Surveillance téléphonique».
Le PFPD a participé à ce groupe d'étude, il a donc eu la possibilité d'y faire valoir ses exigences. Les travaux du groupe d'étude ont débouché sur le projet de loi fédérale sur la surveillance de la correspondance postale et des télécommunications du 2 juin 1997, auquel le PFPD a donné son accord.
Ce projet a été mis en consultation et fut soumis à de nombreuses modifications au cours de la procédure de consultation ainsi que lors de la consultation des offices. Cela signifie que le projet de loi, tel qu'il est présenté aujourd'hui dans le message, ne peut plus recevoir l'appui entier du PFPD.
De l'avis du PFPD, d'importantes exigences qui étaient contenues dans le rapport de la CdG ne sont plus prises en considération dans le projet de loi actuel.
Il faut d'une part penser à l'exigence d'un catalogue restrictif des délits. Le catalogue des délits qui a été retenu ne correspond en aucune manière à l'objectif du catalogue restrictif qui avait été demandé par la CdG, puisque non

seulement les crimes graves mais aussi les simples délits et les contraventions y ont été incluses. Il ne faut pas oublier que la surveillance du trafic postal et des télécommunications constitue une atteinte très grave à la personnalité des personnes concernées, raison pour laquelle cette mesure ne doit être prise que dans des cas de délits graves selon le principe de la proportionnalité.
Nous étions d'avis à l'époque que les exigences de la protection de la personnalité pouvaient être suffisamment respectées même sans l'adoption d'un catalogue restrictif des délits dans les cas où la surveillance était dictée par une présomption grave d'avoir commis un crime ou un délit susceptible d'être punis comme crime, dans les cas graves ou en présence de critères particuliers. Ceci limiterait la surveillance aux crimes graves et réduirait fortement le nombre des délits pour lesquels une surveillance pourrait être ordonnée. L'inclusion dans le catalogue des délits d'actes que le législateur considère purement comme simples délits ou comme contraventions n'est en aucun cas justifiable.
En plus de la restriction de la surveillance aux crimes ou aux délits susceptibles d'être punis comme crimes, dans les cas graves ou en présence de critères particuliers, initialement prévue dans le projet du 2 juin 1997, il y avait également la condition que la gravité ou la nature du délit justifie la surveillance, notamment dans les cas où une présomption existe que le délit est commis de manière professionnelle, organisée, de manière répétée ou par une organisation criminelle. Le projet de message stipule uniquement que la gravité du délit doit justifier la surveillance. La restriction concernant le caractère professionnel, organisé, répété ou lié à une organisation criminelle a été supprimé. Les exigences initiales du rapport de la CEP pour une application plus restrictive de la surveillance téléphonique ont ainsi été complètement délayées dans le projet actuel.
D'autre part, en rapport avec l'utilisation de «Natel easy», une disposition a été incorporée dans le projet de message stipulant que l'autorité compétente peut autoriser, dans les cas où un raccordement change fréquemment, que tous les raccordements identifiés utilisés par la personne suspecte puissent être surveillés sans qu'une autorisation individuelle soit nécessaire dans chaque cas. Cette disposition a pour effet que tous les raccordements de personnes tierces (exemple: la personne suspecte passe deux nuits à l'hôtel, une nuit chez un ami, trois nuits chez sa mère et entre deux elle utilise un «Natel easy», etc.) peuvent également être surveillés sans nécessiter d’approbation. L'exigence de la CdG d'améliorer la protection de personnes tierces n'est ainsi non seulement pas du tout prise en compte, mais en plus la protection est fortement réduite puisqu'il suffit de signaler à l'autorité d’approbation qu'une surveillance a eu lieu.
En outre, il est prévu que les fournisseurs de services de télécommunication soient obligés de conserver pendant une durée de six mois les données existantes pour l'identification de l'abonné ainsi que les données relatives aux communications et à la facturation, les données relatives à la correspondance postale même pendant «au moins» six mois.

Le traitement (en particulier la saisie et la conservation) de ces données par les prestataires de services a lieu pour l'établissement des communications ainsi que pour l'établissement des factures. Les dispositions qui sont prévues régleraient ainsi la durée de conservation pour une nouvelle finalité, à savoir celle d'une poursuite pénale. Déjà dans l'ordonnance actuelle sur les services de télécommunication (OST), une disposition complémentaire a été introduite dans ce sens – sans nous consulter préalablement – disposition qui devrait maintenant être érigée au niveau d'une loi. Une telle disposition transforme cependant la conservation de ces données à un traitement préventif de données à l'intention des autorités de poursuite judiciaire. Cela signifie que les données ne sont plus traitées exclusivement en rapport avec une instruction judiciaire concrète. Ces données sont plutôt mises à disposition des autorités de poursuite judiciaire indépendamment du fait qu'un délit ait concrètement été commis. De cette manière, les données accessoires de communication de l'ensemble de la population suisse sont conservées à titre préventif dans un but de poursuite judiciaire.
A part les points critiqués par nous-mêmes, d'autres experts ont également émis des avis très critiques sur le projet de message. Ceci a eu pour effet que la Commission juridique du Conseil national a décidé lors de sa séance du 27 novembre 1998, d'instaurer une sous-commission chargée d'élaborer un contre-projet avec l'appui d'experts. Ce contre-projet devrait notamment prendre en compte la protection des droits fondamentaux ainsi que les exigences de la protection des données, proposer principalement les modifications de loi qui découlent nécessairement de la libéralisation du marché des télécommunications et garantir la protection du secret professionnel et du droit à refuser de témoigner ainsi que les droits d'accès, de consultation et de contrôle entérinés aux articles 8 et 13 de la Convention européenne des droits de l'homme.

1.2. Création de bases légales pour des registres de personnes à l'Office fédéral de la police

Afin de respecter la période transitoire de la LPD octroyée aux organes fédéraux pour créer des bases légales suffisantes pour leurs traitements de données personnelles sensibles et de profils de la personnalité, l'Office fédéral de la police a soumis au Parlement un paquet de lois.

Les organes fédéraux sont tenus, dans un délai de transition de cinq ans à compter de l'entrée en vigueur de la LPD, de créer les bases légales suffisantes pour les traitements existants de données sensibles et de profils de la personnalité. C'est pourquoi l'Office fédéral de la police (OFP) a soumis un gros paquet de lois (TGV) pour examen au Parlement (voir aussi le 5^{e} rapport

d'activités, page 149 ss). Ce paquet de loi comprend entre autres la révision de l'art. 11 al. 1 de la loi fédérale sur les offices centraux de police criminelle de la Confédération du 7 octobre 1984 (LOC). La version actuellement encore en vigueur autorise le Conseil fédéral à ordonner qu'un office central exploite une base de données pour l'accomplissement de ses tâches. Cette formulation respecte le principe fondamental de la LOC qui prévoit l'instauration et la gestion d'offices centraux distincts. Selon le nouveau projet, les offices centraux de police exploitent un système de traitement des données commun pour l'accomplissement de leurs tâches. Cela signifie que toutes les données qui sont traitées par les divers offices centraux de police criminelle de la Confédération sont mises dans le même «gros sac». Cette version avait été acceptée par la Commission juridique du Conseil des Etats. La Commission juridique du Conseil national par contre s'est prononcée contre la création d'un système central d'informations personnelles en matière de police. Elle a renvoyé le projet au Conseil fédéral en lui demandant d'élaborer un concept global pour la fusion des fichiers des offices centraux qui inclue l'organisation et qui satisfasse aux exigences de la protection des données.
Nous avions jusqu'ici toujours défendu notre point de vue envers l'OFP ainsi que dans les délibérations des commissions juridiques que la réorganisation des services des offices centraux entreprise par l'OFP n'était pas conciliable avec la LOC, étant donné que cette dernière prévoyait des offices centraux de police criminelle distincts, gérés séparément. Nous étions en outre d'avis que la révision prévue de l'art. 11 al. 1 LOC n'était pas apte à légaliser les états de fait créés par l'OFP. C'est pour cette raison que nous sommes satisfaits de voir que le projet a été renvoyé, au moins dans la mesure ou ceci rend nécessaire une révision plus poussée de la LOC.

1.3. Visite auprès du service de contrôle des systèmes DOSIS et ISOK de l'Office fédéral de police

A l'occasion d'une visite auprès du service de contrôle de l'Office fédéral de police pour les systèmes informatiques DOSIS et ISOK, nous avons eu la possibilité de nous faire une idée des méthodes de travail dans ce service et de poser des questions que nous avions préalablement préparées.

L'Office fédéral de la police (OFP) exploite un service de contrôle pour les systèmes de traitement de l'information DOSIS et ISOK. A l'occasion de deux visites effectuées en deux matinées, nous avons pu nous faire une idée des méthodes de travail dans ce service. Nous avons constaté que le service de contrôle doit remplir une tâche à très haute responsabilité. En particulier, il assume une

fonction charnière entre les intérêts des enquêteurs de police et ceux de la protection des données. Il s'est cependant également avéré qu'à beaucoup d'égards les exigences de l'enquête policière et de la protection des données se recoupent. Ceci vaut en particulier pour l'exigence que les données soient correctement saisies et traitées, ce qui englobe autant l'exactitude du contenu que l'actualité temporelle. L'exigence de l'exactitude des données est entre autres absolument nécessaire dans le cadre des activités d'analyse policière, tout en étant un des principes de toute première importance de la protection des données.

La visite nous a également permis de poser des questions relatives
- au traitement de données personnelles dans les systèmes DOSIS et ISOK;
- à la reprise de données personnelles de l'index central des dossiers ZAN dans les systèmes DOSIS et ISOK;
- aux tâches confiées au service de contrôle ainsi qu'aux
- dispositions dans les ordonnances et les règlements sur le traitement des données dans les systèmes DOSIS et ISOK.

Notre visite a fourni les résultats suivants:
- Avec la mise en place du système de traitement des données ISOK au 1er janvier 1998, les données personnelles qui concernent le crime organisé et qui étaient stockées dans l'index central des dossiers ZAN, ont pu être reprises dans le système ISOK. La reprise des données s'est effectuée telle quelle à l'aide d'un programme batch sans que le service de contrôle vérifie préalablement si les données étaient conformes aux dispositions légales. Cette démarche a été motivée par le volume des données, par l'effort de travail à fournir de la part du service de contrôle vu ce volume de données ainsi que le manque de «matière première», à savoir les dossiers correspondants aux données et qui auraient permis de vérifier la conformité avec la loi des données reprises. La conséquence de cette démarche est que les données ne sont pas conformes à la loi et qu'elles sont dans un très mauvais état. Les données ont été stockées dans une nouvelle catégorie de données «KA», catégorie qui n'est prévue ni dans l'ordonnance ISOK, ni dans le règlement de traitement ISOK et qui n'est donc pas défendable du point de vue légal. Afin de limiter cet état de fait non conforme à la loi, il avait été prévu à l'origine de ne stocker dans cette catégorie «KA» que les données qui avaient été transférées dans l’index central des dossiers ZAN vers le système ISOK avant le 21 juin 1998. Nous avons cependant dû constater que des utilisateurs continuent à saisir des données dans la catégorie «KA» après la date du 21 juin 1998.
  La vérification par le service de contrôle ne se fait que dans des cas isolés, dès que des nouveaux faits sont signalés concernant des données de base. Le service de contrôle vérifie alors sur la base des informations reçues ainsi que sur la base des dossiers existants si les données peuvent être enregistrées dans

le système ISOK. Si le service de contrôle constate que la saisie de ces données n'est pas autorisée, ces dernières sont supprimées. Cette démarche a pour effet que les informations qui existent actuellement dans la catégorie «KA» ne sont pas vérifiées en ce qui concerne leur conformité avec la loi aussi longtemps qu'il n'y a pas de nouveaux faits. Cela signifie que des données subsistent pendant des années dans ce système sans être vérifiées par le service de contrôle et que des données qui devraient être qualifiées de «non vérifiées» sont mises à disposition des utilisateurs au-delà des délais de conservation prévus par l'ordonnance ISOK.
Il était d'autre part prévu que toutes les données visées de la catégorie «KA», munies de la catégorie d'accès restreinte prévue dans le règlement de traitement ISOK, seraient transférées dans le domaine «crime organisé» dès que cette fonction deviendrait disponible. Nous partageons l'avis que toutes les données stockées dans la catégorie «KA» doivent être soit vérifiées d'ici le 21 juin 2000 au plus tard, soit supprimées comme étant non vérifiées à cette même date.

- L'art. 2 lit. e du règlement de traitement ISOK prévoit une gestion des dossiers et des documents dans le système ISOK. Chaque antécédent est référencé par le numéro de dossier. En principe, nous n'avons rien à redire à ce sujet. Contrairement au système DOSIS, le système ISOK contient cependant des enregistrements de base à des fins de gestion des dossiers et des documents pour lesquels il n'existe pas d'antécédents proprement dits dans le système même. L'enregistrement d'antécédent est simplement saisi avec une référence vers le dossier papier et contient des informations nécessaires pour la gestion du dossier. Les enregistrements d'antécédents ne contiennent donc pas de données selon l'ordonnance ISOK. De plus, le fait de gérer les dossiers et documents dans le sous-système «Personnes et antécédents», cause un problème au niveau des délais d'effacement des données. Les enregistrements de ce sous-système sont soumis aux durées de conservation des données stipulées pour le sous-système en question dans l'ordonnance ISOK, à savoir 2 ans pour les données peu fiables et dix ans pour les données fiables.
  Une telle gestion des dossiers et des documents n'est pas conciliable avec l'ordonnance ISOK, d'autant plus qu'il est possible de tenir un contrôle des affaires et des délais dans un autre sous-système. Elle doit donc ne plus avoir lieu.

- L'art. 3 al. 4 du règlement de traitement ISOK stipule que les informations qui ne remplissent ni les conditions de l'al. 2, ni celles de l'al. 3, peuvent néanmoins être stockées dans le système ISOK si elles concernent une personne ou une organisation pour laquelle il existe déjà un enregistrement de base dans le sous-système «Personnes et antécédents». Cette disposition permet de saisir dans le système ISOK tous les agissements d'une personne qui n'ont aucun

rapport avec le crime organisé, que ce soient des affaires de simple police, des infractions, etc. Ceci peut mener à une situation où l'information relative au crime organisé qui a l'origine était peu fiable est effacée conformément à l'ordonnance ISOK, mais où l'information qui ne présente aucune pertinence en matière de crime organisé continue cependant à être traitée. L'alinéa 4 doit donc être précisé dans le sens que seules peuvent être saisies les informations qui en soi ne sont pas pertinentes en matière de crime organisé, mais qui peuvent jouer un rôle important pour les enquêtes. D'autre part, il doit pouvoir être garanti que lors de l'échéance des délais de conservation des données pertinentes en matière de crime organisé, ces informations soient également effacées du système afin d'éviter qu'un enregistrement de base ne contienne plus que des informations qui ne présentent aucune pertinence en matière de crime organisé.
L'art. 3 al. 4 a pour conséquence que la nécessité d'une pertinence en matière de crime organisé est contournée.

- On enregistre dans le système ISOK des enregistrements de base et des antécédents qui proviennent de sources extérieures (presse, etc.) sans qu'ils ne présentent aucun lien avec un délit. Sont ainsi enregistrés des informations qui concernent des personnes se trouvant dans l'entourage d'une autre personne qui est présumée appartenir au crime organisé, sans que ces informations n'aient elles-mêmes un rapport avec un événement pertinent. A notre avis, ceci constitue un traitement de données inadmissible qui ne doit plus se reproduire.

- On enregistre constamment de nouveaux antécédents contenant les même informations, ce qui mène à des redondances. La conséquence en est qu'il devient difficile de vérifier l'actualité des données qui est un aspect de l'exactitude des données. Il faudrait donc pour cette raison éviter dans la mesure du possible les redondances.

- Près d'un tiers des données enregistrées dans le système DOSIS sont des données peu fiables. Certains cantons saisissent uniquement des données fiables. L'appréciation si les données peuvent être considérées comme fiables ou peu fiables se fait d'un point de vue strictement policier.
Pour qu'une donnée soit *fiable*, un lien direct doit exister avec un cas de stupéfiants. Un cas concret existe si une arrestation a eu lieu, si des drogues ont été confisquées, si une plainte a été déposée, si la police a rédigé un rapport, si une surveillance téléphonique a été ordonnée. Sont considérés comme *données peu fiables* les annuaires trouvés lors de perquisitions, les données programmées dans un PC, un téléphone mobile ou autre appareil de téléphone, des conversations téléphoniques mentionnées, mais non écoutées, étant donné que ces dernières ne révèlent encore rien sur le contenu des conversations.

Dans le système ISOK, on ne dispose pas de critères aussi clairs puisque dans le domaine du crime organisé on n'effectue en règle générale pas de plaintes, dactyloscopies, perquisitions, etc. Parfois on n'entame même pas de procédure d'enquête judiciaire. Ainsi on saisit par exemple comme *donnée fiable* la société qui a beaucoup de dépenses, mais pas de recettes parce qu'elle ne propose pas de produits ou de services. Dans un tel cas, on gère également un enregistrement de base sur les membres du conseil d'administration. On saisit également des données de base sur chaque personne qui a fait une demande de visa.
Il n'existe cependant pas de critères clairement définis pour différencier entre «fiable» et «peu fiable».
Etant donné que le délai de conservation de 2 ans pour les données peu fiables dans le domaine du crime organisé est trop court, on tend à appliquer des critères pas trop restrictifs afin de pouvoir classer les données comme étant fiables.

- On saisit dans le système ISOK des données de base concernant des ressortissants russes qui ont commis des délits de simple police tels qu'un vol dans un supermarché ou l'entrée clandestine dans notre pays. Une telle saisie, effectuée sans qu'il n'existe aucun lien perceptible vers le crime organisé, n'est pas admissible. D'autre part, on enregistre même des ressortissants russes simplement parce qu'ils dépensent leur argent à la rue de la Gare à Zurich ou à St Moritz.
  A notre avis, le simple fait qu'un ressortissant russe dépense de l'argent ne permet pas d'en déduire une pertinence pour le domaine du crime organisé. C'est pourquoi nous considérons qu'un enregistrement de ces données dans le système ISOK n'est pas justifiable. De telles données doivent donc être supprimées.

- Conformément au règlement de traitement, le service de contrôle assure que les «*données saisies dans le système ISOK sont exactes ...*». Il s'agit là d'un contrôle matériel. L'exactitude des données saisies est vérifiée d'une part sur la base des documents écrits existant à l'OFP. Cela signifie par exemple que dans le cas d'informations reçues par le canal d'Interpol, les données saisies sont comparées à celles figurant sur le document papier. Si l'on découvre des inexactitudes, les données sont corrigées. Si aucun document écrit n'existe au sein de l'OFP et que les documents existent auprès des cantons, on procède éventuellement à une vérification des documents lors d'une inspection. Un tel contrôle n'est pourtant effectué que de manière ponctuelle et non pas pour chaque enregistrement. De telles inspections n'ont à ce jour encore jamais été faites (ceci est également vrai pour le système DOSIS). Il en résulte que l'exactitude des informations qui existent sous forme de document papier auprès des cantons n'est pas vérifiée ou ne peut pas être vérifiée.

- Le règlement sur le traitement des données ISOK stipule que le service de contrôle garantit que le système est utilisé en conformité avec les dispositions légales. Il est un fait établi que le service de contrôle ne peut pas donner une telle garantie. Il peut tout au plus instruire et former les utilisateurs, édicter des directives pour le traitement des données dans le système. Il ne peut cependant pas garantir que les utilisateurs respectent les dispositions légales. La seule chose qu'il pourrait éventuellement prévoir, c'est que l'accès au système soit automatiquement bloqué pour les personnes qui violent systématiquement les instructions concernant l'utilisation du système.

L'OFP nous a assuré que toutes les mesures seront prises ou entamées d'ici la fin 1999 pour régler tous les problèmes encore en suspens.

1.4. Ordonnance relative au système de traitement des données pour la lutte contre le faux-monnayage, la traite des humains et la pornographie

Avec la mise sur pied du système de traitement des données pour la lutte contre le faux-monnayage, la traite des humains et la pornographie et avec l'élaboration de l'ordonnance nécessaire du Conseil fédéral, on tente de satisfaire au principe de séparation ancré dans la loi fédérale sur les offices centraux de police criminelle.

Conformément à la loi fédérale sur les offices centraux de police criminelle de la Confédération du 7 octobre 1984 (LOC), les systèmes de traitement des données des offices centraux de police criminelle de la Confédération doivent être gérés séparément des autres systèmes de traitement des données de la police ou de l'administration. L'Office fédéral de la police (OFP) traitait dans son Index central des dossiers ZAN non seulement des données administratives, mais également des données relatives à des enquêtes dans le domaine du faux-monnayage, de la traite des humains et de la pornographie. Afin de satisfaire au principe de la séparation ancré dans la LOC, l'OFP a élaboré – longtemps après l'entrée en vigueur de la loi – une ordonnance sur le système de traitement informatisé pour la lutte contre le faux-monnayage, la traite des humains et la pornographie (FAMP). Ce système a été conçu comme base de données sœur des systèmes de traitement des données en matière de lutte contre le trafic illicite de stupéfiants DOSIS et contre le crime organisé ISOK. Alors que le système DOSIS ne traite que des données concernant le trafic de stupéfiants, la base de données FAMP regroupe des informations relatives à des délits dans les domaines faux-monnayage, traite des êtres humains et pornographie. Dans le cadre de la consultation des offices, nous avions stipulé qu'à notre avis le

système FAMP n'était pas conforme à la LOC. Contrairement à la poursuite du traitement des données personnelles des services des offices centraux dans l'index central des dossiers ZAN, la mise sur pied et l'exploitation du système FAMP soulève à notre avis moins de réserves d'ordre juridique.
L'index central des dossiers ZAN comprend une multitude de conteneurs de données très différents. Il gère des données personnelles pour le service d'identification, pour Interpol ainsi que pour les offices centraux. D'une part, l'index central des dossiers ZAN ne repose pas sur des bases légales suffisantes sous forme de loi au sens formel. Celle–ci ne sera créée qu'après l'adoption du paquet de lois TGV (cf. ci-dessus, «1.2. Création de bases légales pour des registres de personnes à l'Office fédéral de la police») qui doit entrer en vigueur au plus tard au début de 2001. D'autre part, l'index central des dossiers ZAN ne satisfait pas au principe de séparation inscrit dans la LOC.
Le système FAMP par contre est en mesure – par la création de sous-systèmes adéquats – de satisfaire à ce principe de la séparation et ainsi également de respecter le principe de la proportionnalité en matière de protection des données par des dispositions réglant l'accès. En outre, le système FAMP anticipe pour une partie des offices centraux sur la révision de l'art. 11 al. 1 avant-projet LOC (cf. ci-dessus «1.2. Création de bases légales pour des registres de personnes à l'Office fédéral de la police») qui prévoit un système de traitement des données commun pour les services des offices centraux.
Dans le cadre de la consultation des offices, nous avions présumé que le système FAMP prenait en compte le concept de la loi sur les offices centraux et que les bases légales pour un système de traitement des données commun, conforme au concept de la loi sur les offices centraux, entrerait en vigueur au plus tard dans deux ans. Vu sous cet angle, le système FAMP soulève moins de réserves du point de vue juridique et technique que l'index central des dossiers ZAN. Avec le renvoi du projet de révision de l'art. 11 al. 1 LOC par la Commission juridique du Conseil national, l'évolution vers un système de traitement des données commun et la question liée des bases légales est à nouveau remise en question.

1.5. Traitement de données personnelles à l'index central des dossiers ZAN conformément à la loi sur les stupéfiants

Selon la loi fédérale du 3 octobre 1951 sur les stupéfiants, tous les jugements, prononcés administratifs ayant un caractère pénal et ordonnances de non-lieu ainsi que toute poursuite pénale pour violation de la loi sur les stupéfiants de l'Office central de lutte contre le trafic illicite de stupéfiants doivent être communiqués au Ministère Public de la

Confédération, à l'intention du Conseil fédéral. Ces données ont été mémorisées auprès de l'Office fédéral de la police dans l'index central des dossiers ZAN.

L'Office fédéral de la police (OFP) a mémorisé dans l'index central des dossiers ZAN des jugements, prononcés administratifs ayant un caractère pénal et ordonnances de non-lieu relatifs à des violations de la loi fédérale du 3 octobre 1951 sur les stupéfiants (LStup) (cf. art. 12 lit. m de l'ordonnance du 1er décembre 1986 concernant le Service d'identification de l'Office fédéral de police). L'art. 28 al. 2 LStup prévoit cependant que tous les jugements, prononcés administratifs ayant un caractère pénal et ordonnances de non-lieu doivent être communiqués immédiatement après avoir été décrétés, en expédition complète, au Ministère public de la Confédération, à l'intention du Conseil fédéral. Le destinataire est donc le Ministère public de la Confédération. L'art. 12 lit. m de l'ordonnance concernant le Service d'identification est un vestige des temps où le Bureau central suisse de police faisait encore partie du Ministère public de la Confédération. En 1992, le Bureau central suisse de police a été incorporé à l'OFP. La base légale nécessaire sous forme d'une loi au sens formel pour une communication des jugements, prononcés administratifs ayant un caractère pénal et ordonnances de non-lieu relatives aux violations de la LStup à l'OFP et ainsi pour un traitement dans l'index central des dossiers ZAN fait défaut.
Suite à notre intervention, l'OFP nous a confirmé que ces données avaient été supprimées dans le système ZAN.

Conformément à l'art. 29 al. 3 LStup, les cantons sont tenus de signaler tout poursuite pénale engagée pour violation de la LStup à l'Office central de lutte contre le trafic illicite des stupéfiants. Ces communications ont été stockées et traitées par l'OFP dans l'index central des dossiers ZAN. L'ordonnance concernant le Service d'identification de l'OFP, qui règle les traitements de données de l'index central des dossiers ZAN, ne contient cependant aucune disposition qui autoriserait un traitement de ces communications. Cela signifie qu'un tel traitement est contraire à la loi. Nous avions dans ce sens demandé à l'OFP de supprimer toutes les données personnelles communiquées par les cantons ainsi que de supprimer les accès en ligne de personnes qui ne travaillent pas à l'Office central de lutte contre le trafic illicite des stupéfiants. L'OFP a répondu à nos exigences dans les délais.
L'Office central de lutte contre le trafic illicite des stupéfiants utilise pour son travail une statistique sur les stupéfiants. Cette statistique ne présenterait cependant pas la même utilité si elle ne contenait que des données anonymisées. C'est pourquoi l'OFP a proposé de mettre sur pied une base de données séparée pour la statistique sur les stupéfiants, à laquelle seules deux personnes chargées de gérer cette statistique auraient accès. La base légale nécessaire pour une telle

statistique serait immédiatement entamée. Nous avons pu donner notre accord à cette proposition et à cette démarche.

1.6. Accès des établissements pénitentiaires au système RIPOL

Nous avions à traiter une demande émanant du préposé à la protection des données du canton de Zurich concernant le formulaire de visite d'un établissement pénitentiaire. Il s'agissait concrètement de répondre à la question si un établissement pénitentiaire a le droit ou non de consulter le système de recherches informatisées de police RIPOL.

Le préposé à la protection des données du canton de Zurich s'était adressé à nous avec la question si les accès d'un établissement pénitentiaire sur le système de recherches informatisées de police RIPOL était prévu dans les bases légales correspondantes et si ce système constituait un «casier judiciaire».
A l'origine de la lettre du préposé cantonal à la protection des données se trouvait la demande d'un citoyen concernant un formulaire de visite d'un établissement pénitentiaire. Ce formulaire de visite contenait une clause par laquelle la personne signataire autorisait l'établissement à prendre des renseignements sur elle auprès des autorités responsables du casier judiciaire. Les recherches du préposé cantonal à la protection des données révélèrent cependant que l'établissement pénitentiaire ne demandait pas des extraits du casier judiciaire, mais procédait plutôt à des consultations dans le système RIPOL.
Après examen des bases légales existantes, nous somme arrivés à la conclusion que ces dernières ne suffisent pas à justifier un accès en ligne d'un établissement pénitentiaire au système RIPOL.

1.7. Caméra vidéo dans le tunnel du Baregg – AFNES

La police argovienne a installé des caméras vidéo dans le tunnel du Baregg sur l'autoroute A1 entre Zurich et Berne. Ces caméras devaient permettre de tester un système automatisé d'identification de numéros de plaques de véhicules. L'objectif poursuivi par ce projet est d'améliorer la recherche de véhicules.

En juin 1998, alors qu'il était déjà en cours, nous avons été informés par un journaliste du projet test, limité à quelques mois, «Système automatisé d’identification de numéros de plaques de véhicules» (AFNES) de la police

cantonale argovienne. Selon un communiqué de presse du 10 juin 1998 de la Commission technique de police suisse (CTPS), qui est un organe de la Conférence des commandants des polices cantonales de Suisse et de l'Association suisse des chefs des polices locales, ce système a été développé pour optimiser la recherche de véhicules. Ces tests qui on été exécutés en collaboration étroite entre les corps de police et le centre de calcul du Département fédéral de justice et police devaient démontrer l'aptitude pratique de tels systèmes.

Les caméras vidéo installées dans le tunnel du Baregg enregistrent les numéros de plaque de tous les véhicules qui traversent le tunnel et les comparent avec la base de données du système de recherches informatisées RIPOL exploité par l'Office fédéral de la police. Les caméras ont été installées de manière à ce que l'angle de prise d'image soit limité au secteur de la plaque d'immatriculation et qu'il ne soit donc pas possible de voir les occupants du véhicule sur la prise de vue. Etant donné que la vérification se fait immédiatement, ce système pré-suppose un accès en ligne du système AFNES au système RIPOL.

Sur la base de ces faits, nous avons – en qualité d'organe de contrôle compétent pour les fichiers exploités par des organes fédéraux – été invité par la CTPS à une démonstration du système. Sur la base de cette visite et d'examens effectués par la suite, nous avons constaté que les exigences que nous avons formulées pour le domaine qui est de notre compétence – la comparaison avec les données mémorisées dans le système RIPOL – sont remplies:

- la comparaison des numéros de plaque filmés par caméra vidéo avec la base de données RIPOL est effectuée exclusivement dans les buts qui sont définis dans l'art. 2 lit. f et g de l'ordonnance sur le système de recherches informatisées du 19 juin 1995;
- les numéros de plaque enregistrés ne sont mémorisés dans le système que pour la durée de temps qui est absolument nécessaire pour effectuer la comparaison;
- un contrôle pouvant avoir lieu à tout instant de la part de l'Office fédéral de la police ou des instances compétentes de protection des données (cantons, Confédération) est assuré.

Nous avons en outre retenu qu'une nouvelle appréciation du système devrait être faite par nos soins – pour autant que cela fasse partie de nos compétences – si le système devait être mis en service à différents emplacements simultanément et qu'un échange automatique des résultats de la comparaison entre les différents emplacements était prévu.

1.8. Transfert de données en provenance du fichier «Carte d'identité» vers le système de traitement de texte Word

A l'occasion d'une démonstration du fichier «Carte d'identité» (fichier CI), nous avons constaté qu'il était nécessaire à des fins d'impression d'importer des données en provenance du fichier CI dans le système de traitement de texte Word.

La section «Documents d'identité» de l'Office fédéral de la police nous a, une matinée durant, présenté le fonctionnement de ce service ainsi que le fichier CI qu'elle utilise. Nous avons pu nous convaincre des bonnes méthodes de travail ainsi que de la haute conscience des responsabilités des collaborateurs compétents. En ce qui concerne la sécurité des données, le système a présenté un point qui pose problème: le fichier CI n'offre pas de fonction d'impression, il n'est donc pas possible avec ce système d'imprimer des données directement. Si l'on désire donc transmettre par exemple par fax des données du fichier CI à un organe autorisé, ces données doivent d'abord être transférées dans le système de traitement de texte Word d'où elles seront ensuite imprimées sur papier. Une fois que les données se trouvent dans Word, elles peuvent sans autre être modifiées. On pourrait donc par exemple modifier des données d'identification telles que la photo, la signature, le nom, le prénom, la date de naissance, le numéro de carte, la date de délivrance ou même combiner la photo d'une personne avec des données concernant une autre personne, etc.
Suite à notre intervention, le centre de calcul du Département fédéral de justice et police a appliqué des mesures permettant d'une part d'imprimer des données depuis le système pour les envoyer ensuite par fax, d'autre part d'empêcher la possibilité de modifier les données, ce qui améliore la sécurité de ces dernières.

1.9. Transmission non chiffrée de communications de soupçons de blanchiment d'argent par fax

Pour des raisons de protection de la personnalité, il est nécessaire de prendre des mesures organisationnelles et techniques pour éviter autant que possible des abus lors de la transmission d'argent au bureau de communication de soupçons concernant le blanchiment.

Basé sur la loi fédérale pour la lutte contre le blanchiment d'argent, le Bureau de communication en matière de blanchiment d'argent est entré en fonction le 1er avril 1998. Ce bureau de communication est géré par l'Office central de lutte contre le crime organisé auprès de l'Office fédéral de la police. Pour accomplir

ses tâches, le Bureau de communication se sert du système de traitement des données en matière de lutte contre le blanchiment d'argent (GEWA), un système où l'on s'est efforcé de respecter dans une grande mesure les exigences de la protection des données. A l'occasion d'une démonstration, nous avons cependant dû constater que toutes les communications de soupçons faxées au Bureau de communication étaient reçues de manière non chiffrée sur un unique et même numéro d'appel et que le Bureau de communication les retransmettait également de manière non chiffrée aux autorités pénales.
A notre avis, des communications concernant des soupçons de blanchiment d'argent sont des données sensibles au sens de la LPD. De même, les communications du Bureau aux autorités pénales sont également des données sensibles. Nous avons donc informé le Bureau qu'une communication non chiffrée de ces données ne correspondait pas aux exigences de la LPD et de l'OLPD. Nous sommes d'avis que des mesures d'ordre organisationnel et technique doivent être prises qui permettent une transmission des données répondant aux exigences de la LPD et de l'OLPD, que ce soit par fax ou par un autre procédé. Nous avons appris entre-temps de la part du Bureau de communication que des mesures adéquates ont été entamées.

1.10. Ordonnance relative au registre de l'autorité de contrôle en matière de lutte contre le blanchiment d'argent

A part un Bureau de communication en matière de blanchiment d'argent géré par l'Office central de lutte contre le crime organisé de l'Office fédéral de la police, la loi fédérale concernant la lutte contre le blanchiment d'argent prévoit une autorité de contrôle. Cette autorité gère le fichier «Registre des intermédiaires financiers et des organismes d'autorégulation».

L'autorité de contrôle en matière de lutte contre le blanchiment d'argent est une unité faisant partie de l'Administration fédérale des finances. Cette autorité de contrôle doit assumer plusieurs tâches. Ainsi, elle est responsable d'octroyer ou de retirer l'autorisation aux intermédiaires financiers, d'octroyer ou de retirer la reconnaissance aux organismes d'autorégulation; de surveiller les intermédiaires financiers qui lui sont directement soumis et les organismes d'autorégulation; de procéder aux vérifications concernant les intermédiaires financiers non affiliés à un organisme d'autorégulation et n'ayant pas obtenu d'autorisation; de collaborer avec le Bureau de communication en matière de blanchiment d'argent et les autorités de surveillance instituées par des lois spéciales ainsi qu'avec les autorités étrangères de surveillance des marchés financiers, dans les limites de la loi. C'est dans ce but que l'autorité de contrôle

exploite le «Registre des intermédiaires financiers et des organismes d'autorégulation».
En ce qui concerne l'élaboration de l'ordonnance requise, nous avons été consultés à temps. Nous avons pu faire part de nos exigences qui ont été entièrement prises en considération.

1.11. Centrale d'annonce et de transmission de l'Office fédéral de la police

L'Office fédéral de la police gère une centrale d'annonce et de transmission. Au courant des dernières années, nous avons dû intervenir dans plusieurs cas.

Nous avons à plusieurs reprises dû intervenir concernant la centrale d'annonce et de transmission (*Melde- und Übermittlungszentrale - MUZ*) de l'Office fédéral de la police.

- Lors d'une visite auprès de la centrale d'annonce et de transmission, nous avons constaté que le Service de sécurité de l'administration fédérale dépendant du Ministère public de la Confédération (SID) occupait les mêmes locaux que la MUZ. Les collaborateurs du SID accèdent à leur place de travail en traversant les locaux des services des offices centraux (ZSD) pour lesquels ils possèdent une clé. Cela signifie que les collaborateurs du SID peuvent, notamment en dehors des heures de bureau, accéder sans base légale à des données personnelles de la MUZ et des ZSD dont ils n'ont pas besoin pour l'accomplissement de leurs tâches. Etant donné qu'il s'agit en majeure partie de données sensibles, de telles possibilités d'accès doivent absolument être empêchées par des mesures organisationnelles et techniques.

- Les collaborateurs des services des offices centraux peuvent accéder à la centrale d'annonce et de transmission par une porte communicante directe et ainsi se procurer des données personnelles sur simple demande en personne. Afin de prévenir ou de lever toute incertitude concernant ce type de collecte d'information, il est nécessaire de stipuler par écrit les conditions qui régissent une telle communication de données par les collaborateurs de la MUZ à ceux des ZSD et de réglementer l'accès dans des directives. Celles-ci devraient, au moins en ce qui concerne le problème soulevé ici, être édictées sous forme de manuel ayant force de directive, d'ici le milieu de 1999.

- L'Office fédéral de la police avait prévu de publier sur son Intranet des données personnelles ainsi que les photos des collaborateurs de la MUZ contre

leur gré. Etant donné que les collaborateurs de la MUZ d'une part ne figurent pas dans l'annuaire fédéral et que d'autre part ils travaillent dans un domaine touchant à la sécurité qui exige des mesures de protection, il n'est ni proportionnel, ni justifiable de quelque manière que ce soit de diffuser sur l'Intranet les données personnelles, en particulier les photos des personnes concernées. S'ajoute à ceci que des photos peuvent contenir des données sensibles pour la communication desquelles une base légale appropriée doit exister (concernant ce problème, voir aussi en général p. 247).

- Nous avons en outre appris que les communications téléphoniques reçues à la MUZ étaient enregistrées. D'une part se posent les questions si l'enregistrement porte uniquement sur des données accessoires ou sur l'intégralité de la conversation et si d'éventuels transferts des communications à d'autres collaborateurs de l'Office fédéral de la police sont enregistrés. D'autre part, une base légale pour une telle atteinte à la personnalité des personnes appelant la centrale ainsi que des collaborateurs de cette dernière n'existe pas. L'Office fédéral de la police nous a assuré que de tels enregistrements n'auront plus lieu.

- Nous avons également appris que la MUZ traite des affaires pour le compte de la section Interpol. L'Office fédéral de la police a justifié ceci par le fait que la MUZ était à l'origine issue du service radio d'Interpol Suisse et que pour cette raison la tradition veut qu'elle traite également des dossiers Interpol. Même s'il est vrai que la MUZ est issue du service radio d'Interpol Suisse, ceci ne justifie à notre avis pas qu'elle traite des dossiers. La fonction de la centrale d'annonce et de transmission consiste, comme son nom l'indique, exclusivement à distribuer des informations aux instances compétentes. Pour que la centrale traite des dossiers, les bases légales nécessaires selon la LPD pour un tel traitement font défaut. Une attribution de tâches basée sur la tradition ne peut remplacer les bases légales exigées conformément à la LPD.

1.12. Papiers d'identité

Au début 1998, l'Office fédéral de la police a entamé le projet «Nouveau passeport suisse». L'objectif est de créer d'ici l'an 2003 un nouveau passeport ainsi qu'une loi sur les papiers d'identité.

Etant donné que le nombre de falsifications du passeport suisse 85 augmentent, que l'actuel passeport ne permet pas – contrairement aux passeports de la majorité des pays limitrophes – une lecture automatisée et que l'Organisation de

l'Aviation Civile Internationale demande que tout nouveau passeport doit avoir un format déterminé et que sa lecture doit être automatisable, l'Office fédéral de la police a entamé au début 1998 déjà les travaux préliminaires pour un projet «Nouveau passeport suisse». En novembre 1998, le conseiller fédéral Arnold Koller a instauré un groupe de projet. Celui-ci a pour mission de concevoir un nouveau passeport suisse et d'élaborer une loi fédérale sur les papiers d'identité. Le Préposé fédéral à la protection des données est représenté dans ce projet.
Les problèmes du point de vue de la protection des données soulèvent entre autre les questions

- du traitement des données saisies pour établir les papiers d'identité;
- des indications faites dans les papiers d'identité;
- de la lecture automatisée, en particulier quelles sont les données lisibles par la machine, ainsi que du stockage éventuel et de la réutilisation des données lues par la machine;
- de la mise sur pied et de l'exploitation de base de données électroniques;
- des éventuels accès en ligne;
- des délais de conservation et de suppression des données.

1.13. Le projet «Casino 2000»

Jusqu'à l'entrée en vigueur prévue au 1er janvier 2000 de la loi fédérale sur les jeux de hasard et les maisons de jeu, les dispositions d'exécution nécessaires doivent être élaborées. C'est dans ce but que l'Office fédéral de la police a entamé le projet «Casino 2000».

La loi fédérale sur les jeux de hasard et les maisons de jeu a été adoptée par les Chambres fédérales et devrait entrer en vigueur au 1er janvier 2000. Une des conditions nécessaires à cela est en particulier que les dispositions d'exécution nécessaires selon la loi aient été préalablement élaborées, de manière à ce qu'elles puissent entrer en vigueur en même temps que la loi. C'est pour l'élaboration de ces dispositions d'exécution sous forme d'ordonnances du Conseil fédéral que l'Office fédéral de la police a entamé le projet «Casino 2000». Ces dispositions d'exécution concernent entre autres l'instauration de la Commission des maisons de jeu, la définition de la procédure pour l'octroi des concessions pour maisons de jeu, l'élaboration d'un concept social ainsi que d'un concept de sécurité.
Le Préposé fédéral à la protection des données est représenté dans ce projet. Les questions importantes du point de vue de la protection des données sont la question du traitement des données, c.-à-d. de la collecte, du stockage, de la transmission de données personnelles en rapport avec l'accès aux maisons de

jeu. Ainsi, les maisons de jeu sont tenues de vérifier l'identité des personnes avant de leur autoriser l'accès. Il existe une interdiction de jouer pour certains groupes de personnes définis dans la loi. Un de ces groupes de personne est constitué des personnes pour lesquelles une maison de jeu a prononcé une interdiction de jeu. Une maison de jeu peut en outre exclure du jeu toute personne dont elle sait ou doit admettre – sur la base de ses propres perceptions à l'intérieur de la salle de jeu ou sur la base d'informations fournies par des tiers – qu'elles

- sont surendettées ou ne s'acquittent pas de leurs obligations financières;
- risquent des sommes au jeu qui ne sont en aucun rapport avec leurs revenus ou leur fortune;
- entravent l'exploitation normale de la maison de jeu.

Conformément à la loi, la maison de jeu inscrit l'interdiction de jeu dans un registre et communique aux autres maisons de jeu de Suisse l'identité des personnes frappées d'une interdiction. La maison de jeu doit permettre en tout temps aux autorités de poursuite judiciaire de consulter ce registre.
Du point de vue de la protection des données, il est intéressant de relever que les maisons de jeu sont également soumises à la loi sur le blanchiment d'argent.

1.14. Groupe de travail «Politique d'information des autorités de poursuite pénale de la Confédération»

Suite à un postulat de la Commission de gestion du Conseil national pour l'«amélioration de la politique d'information des autorités de poursuite pénale de la Confédération», qui a été reçu par le Conseil fédéral, un groupe de travail a été instauré pour étudier la question.

Le 29 mai 1997, la Commission de gestion du Conseil national soumit un postulat pour «améliorer la politique d'information des autorités de poursuite pénale de la Confédération». Selon le texte du postulat, le Conseil fédéral doit vérifier la politique d'information des autorités de poursuite pénale de la Confédération. Il doit créer des structures qui permettent une coordination et une distinction claire entre l'administration et les autorités de poursuite pénale. Par sa déclaration du 17 septembre 1997, le Conseil fédéral a reçu le postulat qui a été accepté le 10 novembre. Par la suite, le Ministère public de la Confédération (MPC) a été chargé d'élaborer une ébauche de projet pour l'application de ce postulat. C'est sur la base de cette ébauche de projet que le MPC a instaurée un groupe de travail chargé d'étudier plus à fond la question et de proposer des solutions. Le groupe de travail se composait de représentants du Secrétariat général du Département fédéral de justice et police, de l'Office de

l'auditeur en chef, de l'Office fédéral de la police, de l'Office fédéral de la justice, du MPC et du Préposé fédéral à la protection des données.
Nous avons retenu que – en plus des exigences des autorités pénales et de l'intérêt public – les aspects suivants devaient être pris en compte du point de vue de la protection de la personnalité:
basé sur la jurisprudence du Tribunal fédéral, *l'énoncé des faits* communiqués par les autorités doit être vrai, neutre, complet et proportionnel. Tout *jugement* dans une information émanant d'autorités doit être conforme à la réalité et ne doit pas dépasser la limite de la propagande. Le *besoin* d'informer découle d'un intérêt public ainsi que de l'obligation de corriger de fausses informations diffusées dans les médias. L'information émanant des autorités est *limité* par les intérêts privés protégés, en particulier la protection de la personnalité en matière de considération sociale, le respect de la vie privée et de famille, la présomption d'innocence jusqu'à un jugement définitif, le maintien du secret en face de jugements indignes, blessants et inutiles (principe de la proportionnalité). Aucune information permettant d'identifier un avocat, un témoin, un plaignant, une victime, un détenteur de compte, un numéro de compte, un institut financier ne doit être communiquée.
La communication de données sensible à l'étranger (telles qu'elles ont lieu lors de poursuites pénales) n'est autorisée du point de vue de la protection de la personnalité que si elle ne porte pas une atteinte grave à la personnalité de la personne concernée à l'étranger, c.-à-d. en règle générale dans les cas où le pays étranger dispose d'une législation en matière de protection des données équivalente à la nôtre. Ce principe doit être observé lors de demandes émanant de journalistes étrangers. Certaines circonstances, telles que des communiqués de presse qui ont déjà été diffusés en Suisse et auxquels les journalistes étrangers peuvent à tout moment accéder peuvent cependant mener à apprécier la situation de manière différente. Lors de chaque communication de données personnelles sur la base d'autres communications de presse déjà effectuées, il ne faut pas perdre de vue que les communications déjà effectuées dans la presse peuvent constituer des atteintes à la personnalité. Une communication de données personnelles par les autorités de poursuite pénale de la Confédération ne pourrait pas être justifiée compte tenu de telles atteintes à la personnalité.
Nos demandes ont été très bien reçues au sein du groupe de travail. Elles ont été pris en compte dans le rapport final adressé au Secrétariat général du Département fédéral de justice et police. Le travail au sein de ce groupe a néanmoins démontré combien il est difficile de définir une politique d'information à l'aide de règles claires. En tous les cas, il y a lieu de considérer les avantages et les inconvénients des divers intérêts en jeu.

1.15. Projets de privatisation et banques de données de la police

La Conférence des commandants des polices cantonales de Suisse nous a prié de donner notre avis concernant les projets de divers cantons de confier le traitement de leurs bases de données policières à des entreprises privées.

La Conférence des commandants des polices cantonales de Suisse nous a prié de donner notre avis concernant des projets qu'avaient certains cantons de confier le traitement de leurs bases de données policières à des entreprises privées (outsourcing).
Nous avons retenu que la LPD s'applique au traitement de données personnelles par des personnes privées ou des organes fédéraux. Ceci a pour effet que les traitements de données personnelles par des organes cantonaux sont soumis aux dispositions cantonales de protection des données.
Il est cependant plus difficile de répondre à la question concernant l'application de la législation correspondante en matière de protection des données ainsi qu'à la question de la compétence de l'instance de protection des données dans les cas où les traitements de données sont confiés à des entreprises privées dans le cadre d'un contrat d'«outsourcing». D'une part, le droit cantonal de protection des données est applicable, pour autant que les entreprises privées soient liées au droit cantonal en matière de protection des données sur la base de dispositions légales ou contractuelles. L'appréciation de questions relatives à la sécurité des données relève de la compétence de l'organe cantonal de protection des données. D'autre part, les entreprises privées sont soumises à la LPD, ce qui implique la compétence du Préposé fédéral à la protection des données.
Selon les dispositions cantonales, la compétence en ce qui concerne l'outsourcing peut être réglée de différentes manières. Il est donc indiqué que les autorités cantonales se mettent en rapport avec les instances cantonales de protection des données lorsqu'il s'agit de trouver des solutions conformes à la loi pour les traitements de données confiés à des tiers.
Au niveau fédéral, la responsabilité de la protection des données incombe à l'organe fédéral qui traite ou laisse traiter les données dans le cadre de l'accomplissement de ses tâches. Il doit veiller à ce que les données soient traitées conformément au mandat, en particulier en ce qui concerne leur utilisation et leur communication. Cela signifie en outre que les mesures techniques et organisationnelles générales et particulières décrites aux art. 8 et 9 OLPD doivent être remplies par l'entreprise privée. Si l'entreprise tierce n'est pas soumise à la loi fédérale sur la protection des données, l'organe responsable doit s'assurer que d'autres dispositions légales garantissent une protection des données équivalente, à défaut de quoi elle doit garantir cette protection par voie de contrat.

1.16. Exercice du droit d'accès indirect au système ISIS de la police fédérale

Avec l'entrée en vigueur de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, de nouvelles tâches nous ont été confiées dans le cadre des dispositions sur le droit d'accès indirect au système de traitement des données relatives à la protection de l'Etat (ISIS). Toute personne peut en effet nous demander de vérifier si des données la concernant sont traitées conformément au droit par la police fédérale. Après neuf mois d'application de cette nouvelle réglementation, un premier bilan intermédiaire peut être tiré. Ce dernier doit être nuancé selon que l'on se place du point de vue des autorités concernées ou sous l'angle des personnes ayant déposée une demande d'accès.

Le 21 mars 1997, l'Assemblée fédérale a adopté la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Dans le cadre de cette loi entrée en vigueur le 1er juillet 1998, le Parlement nous a attribué de nouvelles tâches légales en nous confiant la mise en application des dispositions relatives au droit d'accès indirect des personnes concernées aux données traitées par la police fédérale.

Jusqu'alors, à l'exception des demandes portant sur des documents de la police fédérale antérieurs à mai 1990 traitées par le Préposé spécial nommé dans le cadre de «l'affaire des fiches», les demandes de consultation de tels documents étaient traitées directement par le Ministère public de la Confédération en vertu des dispositions de l'ordonnance relative au traitement des documents de la Confédération établis pour assurer la sécurité de l'Etat, et de l'ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat (Ordonnance ISIS).

Avec l'entrée en vigueur de l'article 18 LMSI, cette procédure du droit d'accès direct des personnes concernées à leurs données a été remplacée par un mécanisme d'accès indirect exercé par notre intermédiaire. Cette nouvelle disposition est le fruit de longs débats au niveau des Chambres fédérales. Dans un premier temps, le projet prévoyait de reprendre la même réglementation que celle adoptée pour le droit d'accès dans la loi fédérale sur les Offices centraux de police criminelle de la Confédération. Une solution différente a finalement été adoptée par le Parlement. En effet, bien que s'inspirant fortement de l'article 14 de la loi sur les Offices centraux, l'article 18 LMSI a fait l'objet de certains nouveaux aménagements.

Cette disposition prévoit ainsi que toute personne peut nous demander de vérifier si des données la concernant sont traitées conformément au droit dans le système d'information de l'Office fédéral compétent en matière de sûreté intérieure (c.à.d. la police fédérale). Après avoir effectué auprès de la police fédérale ces vérifications, nous communiquons au requérant une réponse au libellé toujours identique selon laquelle aucune donnée le concernant n'a été traitée illégalement ou que, dans le cas d'une éventuelle erreur dans le traitement des données, nous avons adressé à l'Office fédéral la recommandation d'y remédier.

La loi stipule que cette communication n'est pas sujette à recours. La personne concernée peut toutefois demander que la Commission fédérale de la protection des données examine notre communication ou l'exécution de la recommandation que nous aurions émise. La Commission fédérale de la protection des données communique alors à la personne concernée une réponse au libellé toujours identique selon laquelle l'examen a eu lieu conformément au sens de la requête.

Contrairement à la loi fédérale sur les Offices centraux de police criminelle de la Confédération, la LMSI prévoit cependant qu'à titre exceptionnel, en vertu des dispositions de la LPD, nous pouvons fournir de manière appropriée des renseignements aux personnes qui en font la demande, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable.

Enfin, il est prévu que les personnes recensées ayant déposé une demande de renseignements seront renseignées par la police fédérale dès que les intérêts liés au maintien de la sûreté intérieure n'exigent plus le secret, au plus tard lors de l'expiration de l'obligation de conserver les données, conformément à la loi fédérale sur la protection des données, et pour autant que cela n'entraîne pas un volume de travail excessif.

Après neuf mois d'application de cette nouvelle disposition, un premier bilan peut être établi. Ce dernier doit cependant être nuancé selon que l'on se place du point de vue des autorités concernées (PFPD, police fédérale) ou des personnes ayant déposé une demande d'accès.

En tant qu'autorité chargée d'appliquer cette réglementation, nous avons été confrontés à moult problèmes procéduraux et juridiques. En collaboration avec la police fédérale, de nombreuses règles de procédure ont ainsi dû être mises en place afin d'assurer une application adéquate de ce droit d'accès indirect. De nombreuses demandes étant encore directement adressées à la police fédérale, il

a fallu par exemple veiller à ce que ces dernières nous soient transmises sans que cette autorité ne procède à un enregistrement, pour éviter qu'une personne déposant une demande d'accès alors qu'elle n'est pas connue de la police fédérale ne se retrouve ensuite enregistrée dans le système ISIS en raison de sa requête. D'autre part, de nombreuses discussions ont eu lieu avec les représentants de la police fédérale pour mettre au point notre mode de consultation du système ISIS et, des documents des dossiers existant éventuellement sur une personne demanderesse.

Les demandes déposées pour l'instant ont nécessité un investissement important de nos ressources afin d'examiner chaque demande de manière à répondre aux exigences de la LMSI. En effet, après avoir pris connaissance de l'enregistrement ou non de la personne concernée dans le système ISIS, il convient de vérifier, le cas échéant, si les données enregistrées dans ISIS sont traitées conformément au droit. Dans les cas où la personne concernée est bien enregistrée dans le système, nous procédons encore à la vérification des dossiers correspondants. A cet effet, la police fédérale nous fournit alors les documents tirés des différents dossiers papiers auxquels renvoie le système ISIS, afin que l'on puisse procéder à leur examen. Ces étapes achevées, il nous appartient ensuite d'examiner le mode de réponse à transmettre à la personne concernée, afin de déterminer si cette dernière recevra une communication au libellé toujours identique ou si les conditions exceptionnelles mises à une communication plus étendue au sens de la LPD sont remplies dans le cas d'espèce.

Lors de l'examen des différentes demandes que nous avons été amenés à traiter, nous avons en outre émis différentes recommandations à l'attention de la police fédérale afin de faire rectifier certaines erreurs constatées dans le traitement des données. Ceci concernait notamment l'enregistrement de données d'identité incorrectes, ou le protocole d'interrogation et les critères de recherche dans le système ISIS lors de l'examen des demandes d'accès. La police fédérale a suivi nos recommandations en procédant aux rectifications demandées.

Dans le cadre de l'application de cette nouvelle réglementation, un certain nombre de points devront encore être éclaircis, notamment l'étendue du droit d'accès que nous pouvons dans certains cas exceptionnellement octroyer en vertu de la LPD, les voies de droit applicables, la portée des renseignements que devra fournir la police fédérale aux personnes enregistrées à l'expiration des délais de conservation ou à l'échéance des intérêts liés au maintien du secret pour des raisons de sûreté intérieure, les conservation et archivage des dossiers de demandes d'accès.

En se plaçant maintenant du point de vue des personnes concernées, force est de constater que le mécanisme prévu dans la LMSI ne correspond pas à un

véritable droit d’accès. En effet, ces dernières ne peuvent recevoir de notre part en principe qu’une communication au libellé toujours identique, qui ne leur permet pas de savoir si elles sont enregistrées ou non par la police fédérale. Une communication plus étendue est en effet soumise à des conditions très strictes, qui rendent l’application de cette exception très difficile voire impossible.

Contrairement à la situation antérieure où le Ministère public de la Confédération décidait parfois d’indiquer clairement à une personne qu’elle n’était pas enregistrée, le nouveau cadre juridique rend une telle possibilité aléatoire en raison des conditions cumulatives qui doivent être réalisées: nous pouvons fournir des renseignements autres que le libellé toujours identique seulement si cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et s’il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable.

Le mécanisme de consultation mis en place permet en revanche pour les personnes concernées d’avoir la garantie que leur demande a été traitée par un organe extérieur à la police fédérale. En outre notre examen ne se limite pas à voir si une personne est ou non enregistrée par la police fédérale, mais permet de vérifier, le cas échéant, si les traitements de données sont conformes au droit et de faire rectifier les éventuelles erreurs constatées.

En résumé il ressort de ce qui précède que cette tâche supplémentaire qui nous a été confiée est considérable, si l’on veut traiter chaque demande conformément aux exigences de la loi. Cela nous permet en contrepartie d’exercer un contrôle plus régulier sur les traitements de données effectués par la police fédérale. Par contre du point de vue de la personne ayant déposé une demande d’accès, cette surveillance que nous exerçons par le biais du droit d’accès indirect ne doit pas occulter le fait qu’elle ne recevra en principe de notre part pour toute réponse qu’un libellé toujours identique ne lui fournissant aucune indication sur un éventuel traitement de données la concernant.

Il conviendra de voir comment évoluera la mise en application de ce droit d’accès à ISIS pour établir un bilan plus complet (augmentation éventuelle du nombre des demandes, ressources à disposition du PFPD, aspects juridiques et procéduraux pendants, étendue du contrôle du traitement licite des données de la police fédérale, réactions des personnes concernées habilitées à s’adresser également à la Commission fédérale de la protection des données). Il sera alors possible d’analyser la portée réelle et les problèmes concrets liés à ce nouveau mécanisme de consultation des données dans le domaine de la sûreté intérieure.

1.17. Inspection «Online» de la Commission de gestion du Conseil des Etats

Confrontés à la mise en place de liaisons online toujours plus nombreuses permettant à des autorités d'accéder directement à différentes banques de données, nous devons régulièrement rappeler que de tels accès doivent avant tout respecter les principes de proportionnalité, de finalité et d'opportunité. S'inspirant de nos réflexions, la Commission de gestion du Conseil des Etats a effectué une inspection sur cette problématique dans le domaine de la police. Les résultats de ces investigations, auxquelles nous avons participé sous forme d'auditions ou de prises de position écrites, ont été finalisés dans un rapport publié le 19 novembre 1998. Ce rapport met en évidence les lacunes constatées dans la mise en place de ces liaisons et émet de nombreuses recommandations afférentes à la protection des données et au manque de moyens de contrôles qui nous sont attribués.

Nous avons depuis de nombreuses années émis différentes mises en garde concernant les communications de données personnelles par procédure d'appel permettant des accès directs en ligne (online) aux informations. Dans le cadre de notre 1er rapport d'activités, nous avions mis en évidence «les nouveaux dangers» inhérents à la création de bases légales permettant de justifier la mise en place d'un nombre toujours plus impressionnant de liaisons online habilitant de nombreuses autorités à accéder à différentes banques de données (cf. le schéma «online» / rapport d'activités du PFPD 1993/94, p. 91).

Nous avons ainsi rappelé que le respect du principe de légalité vise avant tout un but de transparence, et qu'il ne suffit pas à lui seul à légitimer ces accès. La mise en place d'une liaison online doit en effet être précédée d'un examen de sa nécessité et de sa conformité aux principes de proportionnalité, de finalité et d'opportunité. En d'autres termes, les accès en ligne doivent être conformes aux principes généraux de la LPD et ne peuvent pas uniquement être prévus ou justifiés dans des bases légales.

S'inspirant de nos réflexions, la Commission de gestion du Conseil des Etats (CdG-E) a effectué une inspection portant spécifiquement sur «la mise en place des liaisons online dans le domaine de la police». Elle a ainsi poursuivi les investigations entamées par la Commission de gestion du Conseil national lors du suivi de l'inspection sur l'introduction de l'informatique dans l'administration fédérale au cours de laquelle, en dépit des nombreuses lacunes relevées afférentes à la protection des données, aucun examen approfondi de la surveillance des projets de traitement automatisé n'avait été entrepris.

Se basant sur un rapport d'expertise portant sur différents systèmes informatiques fédéraux de police, la CdG-E a orienté ses travaux sur le respect des principes de la protection des données, les mesures de sécurité, les processus de mise en place des liaisons online ainsi que les mécanismes de contrôle. Durant les différentes phases de cette inspection nous avons été régulièrement consultés, soit au travers d'auditions par la CdG-E elle-même, soit par l'intermédiaire de prises de positions écrites portant sur le rapport d'expertise ou sur le projet de rapport de la Commission.

Le rapport de la CdG-E a été publié le 19 novembre 1998 (cf. site des Services du Parlement http://www.pd.admin.ch). Ce rapport met en lumière les lacunes constatées par la CdG-E dans la mise en place des liaisons online en général, et dans le domaine de la police en particulier. Il contient également un certain nombre de considérations relatives aux contrôles à exercer lors de l'octroi de ces accès en ligne et aux moyens attribués pour les réaliser.

La CdG-E rappelle ainsi que dans le cadre de la surveillance de l'application par les organes fédéraux de la loi fédérale sur la protection des données il est de notre compétence, lors de la mise en place de nouvelles liaisons online, de veiller au respect des principes de proportionnalité, de finalité et d'opportunité. Dans ce contexte, la CdG-E est d'avis que le PFPD manque de moyens, notamment en personnel, pour exercer les contrôles dont il est chargé. La CdG-E précise que ce problème avait déjà été soulevé dans le cadre de l'inspection de la Commission de gestion du Conseil national sur l'introduction de l'informatique dans l'administration fédérale et que cela reste d'actualité.

Sur la base de ces considérations, la CdG-E a émis une recommandation à l'attention du Conseil fédéral prévoyant que ce dernier veille à ce que les liaisons online soient contrôlées de manière plus appropriées par le PFPD. Le contrôle devra garantir que ne sont établies que des liaisons dont la nécessité a été démontrée, dont l'objectif est connu et pour lesquels les risques d'utilisation abusive ou d'atteinte à la personnalité ont fait l'objet d'une évaluation.

Soutenant les démarches de la CdG-E durant son inspection, nous avons également approuvé différentes autres motions et recommandations émises par la CdG-E à l'attention du Conseil fédéral et portant spécifiquement sur plusieurs aspects relevant de la protection des données. Peuvent principalement être citées les motions visant à l'élaboration de réglementations pour les projets pilotes et à l'adoption de normes minimales standard permettant d'améliorer la collaboration entre la Confédération et les cantons lors de l'installation de liaisons online entre autorités fédérales et cantonales (voir aussi page 320 du présent rapport).

De même nous avons exprimé notre soutien aux différentes recommandations de la CdG-E portant notamment sur un examen préalable des accès online sous l'angle des principes de proportionnalité, de finalité et d'opportunité. Le Conseil fédéral est prié quant à lui de faire preuve de plus de transparence dans la formulation des messages accompagnant ses projets de loi, notamment lorsque des liaisons en ligne sont envisagées. La CdG-E recommande en outre la mise en place de procédures décisionnelles uniformes, l'élaboration de principes de base à respecter dans les procédures d'autorisation, un contrôle des délégations de compétence lors de l'octroi des accès en ligne, une augmentation des contrôles de sécurité, ainsi qu'une meilleure surveillance de la fréquence d'utilisation des accès octroyés.

Appelé à se prononcer sur le rapport de la CdG-E ainsi que sur les différentes recommandations qu'il contient, le Conseil fédéral a été invité à faire part de son avis jusqu'en juin 1999.

2. Droit des étrangers et droit d'asile

2.1. Transfert des données du Registre central des étrangers en temps réel

Répondant à une demande de l'Office fédéral des étrangers, nous avons collaboré à la recherche d'une solution visant à régler la problématique du transfert en temps réel des données du Registre central des étrangers avec les cantons de Bâle-Ville et de Genève. Un projet de disposition a en outre été élaboré dans le cadre de la révision en cours de l'ordonnance sur le Registre central des étrangers, fixant de manière précise les conditions strictes d'application de la solution adoptée, tant au niveau de la sécurité que de la protection des données.

L'Office fédéral des étrangers (OFE) nous a demandé de collaborer à l'élaboration d'une solution permettant de régler la problématique du transfert des données du Registre central des étrangers (RCE) en temps réel avec les cantons de Bâle-Ville et de Genève. La solution qui s'est dégagée des contacts entre l'OFE et ces cantons consiste dans la mise en place d'un transfert en temps réel des données du RCE permettant aux cantons de réutiliser leurs propres données, leur évitant ainsi une double saisie.

Nous avons soutenu la nécessité d'élaborer une base juridique ancrant clairement ce transfert des données en temps réel. Nous avons proposé de saisir à cet effet l'opportunité de la révision en cours de l'ordonnance du RCE.

En collaboration avec l'OFE, nous avons dès lors élaboré un projet de disposition réglementant précisément le cadre et les conditions d'utilisation de cette solution. Ainsi, il a été prévu qu'à des fins de rationalisation, une autorité cantonale ou communale chargée du contrôle des étrangers peut transférer en temps réel vers son système d'informations les données du RCE qu'elle a elle-même enregistrées. En outre elle ne pourra traiter ces données pour accomplir des tâches ne ressortant pas du domaine de la police des étrangers que si, indépendamment de ce transfert, le droit cantonal le prévoit expressément. Il a également été précisé que l'OFE devra régler avec les autorités concernées les mesures propres à assurer la sécurité et la protection des données, les directives émises par la Confédération concernant la sécurité informatique étant applicables par analogie. Un renvoi rappelle également les compétences du contrôle cantonal. Enfin ce projet de disposition prévoit que les modalités et charges seront fixées dans un contrat écrit. Ce dernier devra notamment mentionner les mesures de sécurité mises en place, telles que le chiffrement des données ou la journalisation des traitements.

Après consultation des cantons concernés, ce projet de disposition a été introduit par l'OFE dans le cadre de la révision de l'ordonnance RCE. Cette dernière a fait l'objet d'une nouvelle procédure de consultation en décembre 1998, avec pour objectif une entrée en vigueur le 1er mars 1999. Le service de la protection des données de Bâle-Ville nous a fait part dans le courant de janvier 1999 de son soutien à la solution juridique proposée, qui concilie les aspects de praticabilité et de rationalité avec les exigences de la protection des données.

3. Télécommunication et poste

Télécommunication

3.1. Traitement de données personnelles dans le domaine des télécommunications

Avec la libéralisation du marché des télécommunications entrée en vigueur le 1er janvier 1998, les abonnés sont devenus des clients et ont parfois de la peine à s'y retrouver dans la «jungle» de la concurrence. En particulier, ils ne savent pas suffisamment quels sont leurs droits concernant le traitement de leurs données.

Suite à de nombreuses demandes qui nous sont parvenues concernant la protection des données dans le domaine des télécommunications, nous avons décidé de rédiger une brochure d'information sous forme de guide sur ce sujet. Pour l'instant, nous aimerions attirer l'attention sur les dispositions principales de protection des données du droit sur la protection des données ainsi que du droit sur les télécommunications.

Dispositions du droit sur la protection des données

La collecte de données personnelles ne peut se faire que d'une manière licite. Cela signifie qu'une telle action nécessite un motif justificatif, que ce soit sous forme de consentement de la personne concernée ou d'un intérêt prépondérant public ou privé ou d'une loi. Ainsi, la loi prévoit la collecte des données dont un fournisseur de services de télécommunication a besoin pour l'établissement des communications ainsi que pour la facturation de ces dernières. Si par contre, ce dernier désire effectuer d'autres traitements tels que ceux que Swisscom prévoit dans le cadre de son programme client «Joker» (cf. également page 239), il doit obtenir le consentement préalable du client.

Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée, par exemple en écoutant des conversations ou en interceptant des communications.

En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Ainsi, un fournisseur de services de télécommunication est autorisé à traiter le nom et l'adresse de ses clients; il serait par contre disproportionné de demander des informations sur leur situation familiale. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée.

Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre le but qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Ainsi, un fournisseur de services de télécommunication n'est pas autorisé à communiquer les données des abonnés à un contrôle des habitants.

Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. «Exactitude» signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes. «S'assurer» ne signifie cependant pas que les fournisseurs de services de télécommunication sont par exemple responsables à tout moment que l'inscription dans un annuaire soit à jour.

Pour éviter qu'une communication de données personnelles à l'étranger soulève de gros risques d'atteinte à la personnalité de la personne concernée (par exemple suite à une législation en matière de protection des données qui n'est pas équivalente à la législation suisse) et afin de permettre aux personnes concernées de faire valoir leur droit d'accès, la loi prévoit ce qui suit: un fichier doit être annoncé au PFPD avant d'être communiqué à l'étranger dans les cas où la communication n'est pas exigée par une loi et que la personne concernée n'en a pas connaissance.

Par «communication à l'étranger» on entend non seulement la transmission d'un fichier complet ou de parties substantielles de ce dernier, mais également la mise à disposition d'un accès par procédure d'appel (en ligne) ainsi que la transmission à un tiers qui traite les données sur mandat de celui qui les lui a transmises. Un tel cas se présente par exemple lorsque les données d'un presta-

taire suisse sont communiquées à l'étranger pour y être traitées. Est exclu de cette obligation d'annonce la transmission de fichiers à des fins non personnelles, en particulier dans la recherche, la planification et la statistique, pour autant que la forme sous laquelle les données sont publiées exclue toute identification de la personne concernée. D'autre part, une communication vers un pays qui dispose d'une législation en matière de protection des données qui est équivalente à la nôtre ne doit pas non plus être annoncée au PFPD sauf si les fichiers contiennent des données sensibles ou des profils de la personnalité ou s'il est prévu de retransmettre les données vers un autre pays qui ne dispose pas d'une législation en matière de protection des données équivalente.

Un grand nombre de problèmes de la protection des données pourraient être évités si les mesures nécessaires relatives à la sécurité des données étaient prises à temps. Il est également possible de mettre à profit la technique pour remplir les exigences de la protection des données, par exemple en ne traitant que les données qui sont vraiment nécessaires pour le but prévu. Ce qui compte, c'est que l'accès aux données personnelles soit restreint aux seules personnes qui ont en besoin pour accomplir leur tâche.

Le droit d'accès constitue l'élément clé de la protection des données pour la personne concernée, car c'est lui seul qui lui permet de faire valoir ses droits, en particulier en demandant la rectification ou la suppression des données la concernant. Le droit d'accès a d'autre part un effet préventif. Même si ce droit n'est pas souvent exercé, son existence tend à influencer le comportement des maîtres de fichiers pour que ces derniers ne traitent que les données dont ils ont vraiment besoin.

Dispositions du droit des télécommunications

Les fournisseurs de services de télécommunication sont autorisés à traiter les données personnelles des abonnés aussi longtemps et dans la mesure où cela est nécessaire pour l'établissement des communications et pour l'encaissement des rétributions liées à ces prestations.

Le secret des télécommunications est réglé aussi bien dans la Constitution fédérale que dans la loi sur les télécommunications. Il est interdit à toute personne qui a été ou qui est chargée d'assurer un service de télécommunication de donner à des tiers des renseignements sur les communications des usagers (contenus et données accessoires des communications); de même, il lui est interdit de donner à quiconque la possibilité de communiquer de tels renseignements à des tiers. Les fournisseurs de services de télécommunication sont cependant tenus par la loi de fournir aux autorités fédérales et cantonales de justice et de police compétentes qui le demandent des renseignements sur les communications d'un usager lorsque celui-ci fait l'objet d'une poursuite pénale

pour crime ou délit. Cette obligation est applicable dans le même sens dans les cas où le Ministère public de la Confédération, l'Office de l'auditeur en chef ou une direction cantonale de police a ordonné la surveillance des télécommunications dans le but d'éviter un crime ou un délit. Au niveau de l'ordonnance, les fournisseurs de services de télécommunication sont obligés de tenir les données accessoires des communications à disposition des autorités compétentes pour la surveillance des communications pour une durée de six mois. L'obligation de conserver les données de personnes non suspectes pour une durée de six mois au-delà du but initialement prévu et à titre préventif constitue une atteinte grave à la personnalité des personnes concernées. Si l'on tient à poursuivre cette pratique, il faudrait absolument l'institutionnaliser dans une loi au sens formel.

La loi sur les télécommunications actuellement en vigueur laisse aux clients le libre choix de se faire inscrire dans des annuaires. Si un client décide de figurer dans un de ces annuaires, son inscription comporte au moins son nom, prénom ou le nom de sa société, l'adresse et le numéro d'appel. Pour autant qu'il n'y ait pas de risque d'être confondu avec d'autres personnes qui figurent également dans l'annuaire, le prénom ainsi que l’adresse peuvent être inscrits sous forme abrégée sans frais supplémentaires. Toute personne inscrite dans un annuaire peut demander à ce qu'une mention soit apportée indiquant clairement qu'il désire ne pas recevoir d'appels publicitaires et qu'il ne veut pas que ses données personnelles soient utilisées ou communiquées à des fins de publicité directe. Quiconque consulte un annuaire – sous quelque forme que ce soit – doit respecter cette déclaration de volonté. L'éditeur d'un annuaire électronique accessible en ligne doit prendre les mesures nécessaires pour éviter qu'aucune copie n'atterrisse dans un pays qui ne dispose pas d'une législation en matière de protection des données comparable à la nôtre. Il doit prendre les mesures techniques et organisationnelles adéquates pour éviter que le contenu d'une inscription ou une partie de l'annuaire soit modifié ou supprimé.

Le fait qu'il n'est plus obligatoire de se faire inscrire dans les annuaires téléphoniques pose un problème aux services d'appels d'urgence quand il s'agit de déterminer le nom et l'adresse de l'appelant. Swisscom, qui assure aujourd'hui le service universel, avait rendu attentif ses clients l'année passée qu'ils ne pourraient éventuellement plus être identifiés s'ils ne faisaient pas inscrire leur numéro d'appel dans l'annuaire. Il existe cependant une obligation légale d'équiper l'accès aux services d'appels d'urgence de manière à ce que ceux-ci soient en mesure d'identifier l'emplacement de l'appelant. Ceci s'applique de manière explicite également aux abonnés qui ont renoncé à se faire inscrire dans l'annuaire. Aucun abonné à part les services d'appels d'urgence doivent obtenir l'autorisation de voir le numéro de l'appelant si ce dernier a activé la suppression de la transmission de son numéro d'abonné. Les

fournisseurs de services de télécommunication devraient renoncer à utiliser cet argument pour dissuader leurs clients de ne pas s'inscrire dans l'annuaire, ils devraient plutôt assurer l'identification de l'appelant pour les services d'appels d'urgence.

Chaque client est en droit (aussi longtemps qu'il peut contester sa facture) de demander au fournisseur de services de télécommunication de l'informer sur les données qui ont été utilisées pour l'établissement de la facture. Ceci vaut en particulier pour les éléments d'adressage (par ex. le numéro complet qui a été composé), la date et l'heure ainsi que la durée de l'appel de même que le prix de chaque communication. Si un client justifie de manière vraisemblable et par écrit que son numéro a été appelé de manière abusive, le fournisseur de services de télécommunication est tenu de lui communiquer les données suivantes: date et heure de l'appel, numéro d'appel ainsi que nom et adresse de la personne détentrice du raccordement depuis lequel les appels ont été effectués.

Les fournisseurs de services de télécommunications doivent offrir la possibilité à leurs clients d'activer la suppression de leur numéro d'abonné sur l'appareil de l'appelé, aussi bien séparément pour chaque appel que de manière permanente. Ils doivent offrir à l'appelé la possibilité de refuser un appel entrant qui n'affiche pas le numéro de l'appelant. Les fournisseurs de services de télécommunications doivent explicitement attirer l'attention de leurs clients sur l'existence des fonctions cités ci-dessus lors de la signature du contrat d'abonnement.

3.2. Encaissement des redevances de réception des programmes de radio et de télévision

Depuis le 1er janvier 1998, les redevances de réception des programmes de radio et de télévision ne sont plus encaissées par le biais de la facture de téléphone, mais par la société Billag, une filiale de Swisscom. Cette dernière a été mandatée par le Confédération pour encaisser les redevances et doit donc être considérée comme organe fédéral au sens de la loi sur la protection des données.

On a appris dans le courant de l'année 1998 que des données de clients de Swisscom avaient été communiquées à Billag. Cette dernière a utilisé les données pour acquérir de nouvelles personnes soumises à l'obligation de s'annoncer ainsi que pour mettre à jour ses adresses. Ces flux de données furent possibles étant donné que les systèmes informatiques de Swisscom et de Billag n'étaient pas suffisamment séparés. Swisscom n'est cependant pas autorisée à communiquer les données personnelles de ses clients à des tiers sans consentement. Ceci

constitue une extension du but du traitement qui n’est pas manifeste pour les personnes concernées.

Au début 1999, Billag et Swisscom ont séparé leurs système informatiques de manière à ce qu'aucune donnée ne puisse être transférée du système de Swisscom vers celui de Billag. Aucun problème ne se pose pour les données qui ont été publiées dans des annuaires par Swisscom ou par d'autres fournisseurs de services de télécommunication puisque ces données peuvent être utilisées par Billag dans le cadre des tâches que lui confère la loi même si elles contiennent la mention «ne désire aucune publicité».

En rapport avec l'exemption de l'obligation de payer la redevance, nous avons constaté que Billag traitait des données sensibles sans base légale suffisante: toute personne invalide à 50 % au moins, incapable de travailler, disposant d'un revenu modeste ainsi que toute personne touchant l'AVS et disposant d'un revenu modeste peut faire une demande pour être dispensé du paiement des redevances. Les requérants doivent remplir un formulaire assez long pour permettre d'évaluer la situation relative à leur revenu et leur fortune. Ils doivent également joindre un certificat médical ou une décision définitive de l'assurance invalidité concernant leur degré d'incapacité de travail. Ces formulaires sont envoyés à Billag où ils sont conservés. Ils contiennent entre autres des informations relatives à des mesures d'aide sociale ainsi que sur la santé du requérant. Ces données sont sensibles. Un organe fédéral n'est autorisé à les traiter que si une loi au sens formel le prévoit. Actuellement, ce traitement se base uniquement sur une disposition dans une ordonnance. La conformité avec la protection des données doit être rétablie soit par la création d'une disposition appropriée dans la loi fédérale sur la radio et la télévision, soit par une restructuration des flux de données. Celle-ci pourrait être réalisée – dans le sens aussi d'un traitement proportionnel des données – en ne transmettant à Billag que l'information (par ex. depuis l'administration fiscale qui dispose déjà de ces données) que quelqu'un remplit les critères nécessaires pour être exonéré des redevances. Elle n'aurait alors plus besoin des informations détaillées sur le revenu, ni sur l'existence d'une éventuelle invalidité. Dans le cadre de la révision en cours de l'ordonnance sur la radio et la télévision, nous avons rendu attentif l'Office fédéral de la communication à ce problème et proposé une solution sous la forme d'une restructuration des flux de données telle que nous l'avons décrite ci-dessus.

En tant qu'organe fédéral, Billag est en outre tenu d'annoncer tous les fichiers auprès du PFPD pour qu'ils y soient enregistrés.

3.3. Le programme de bonification «Joker» de Swisscom

En février de cette année, Swisscom a mis sur pied un programme de fidélité-client portant le nom de «Joker». Celui-ci permet à un client de cumuler des points de bonification chaque fois qu'il utilise les diverses prestations de Swisscom, points qu'il peut plus tard convertir de plusieurs manières. Il est néanmoins nécessaire d'obtenir le consentement du client dans les cas où le traitement de données va plus loin que la prestation prévue au départ.

Swisscom a pris assez tôt contact avec nous pour éclaircir les questions de protection des données liées à ce programme. Dans une première phase, seuls les chiffres d'affaires qui résultent de l'utilisation des divers services sont cumulés pour chaque client ou pour les personnes vivant dans un ménage. Comme on nous l'a précisé, aucun profil de client n'est établi concernant le comportement en matière de communications. Les données sont cependant utilisées à d'autres fins (évaluations dans le domaine du marketing, statistiques). Ceci nécessite le consentement des personnes concernées qui doivent être clairement informées sur les traitements de données qui sont prévus. Swisscom a rempli ces exigences sur son formulaire d'annonce. Sur la base des informations que Swisscom nous a soumis, nous pouvons dire que le programme est – pour cette première phase – conforme aux dispositions en vigueur de la protection des données.

Pour des raisons de transparence, il serait souhaitable d'apporter les améliorations suivantes qui pourtant ne sont pas obligatoires du point de vue légal: au cas où un client annonce un raccordement pour une autre personne vivant dans le même ménage sur son compte Joker, Swisscom en informe cette personne par écrit en lui donnant la possibilité de contester. Si la personne adressée ne réagit pas, on admet automatiquement qu'elle est d'accord et les points sont portés au crédit du détenteur du compte Joker. Un consentement explicite (opting in) serait certainement préférable du point de vue de la protection des données et pourrait prévenir d'éventuelles réactions négatives.

La question a en outre été soulevée en rapport avec de tels programmes de fidélité-client de savoir dans quelles circonstances les autorités d'enquête sont autorisées à accéder aux données correspondantes des clients. La communication de telles données n'est possible que sur présentation d'une décision judiciaire ou lorsque la personne donne son consentement.

Poste

3.4. GEO-POST – Fichier de données géographiques de la Poste relatives aux bâtiments

La Poste suisse nous a déjà informé en 1997 sur son projet qui consiste à saisir les coordonnées des bâtiments en Suisse. A l'époque, il était question d'un traitement de données non personnelles. Il semble qu'entre-temps d'autres fins d'utilisation soient prévues.

A fin mai 1997, la Poste nous a présenté son projet «Match-GEO». Il s'agissait à l'époque surtout d'optimiser les itinéraires de la Poste, d'offrir des systèmes de navigation à d'autres entreprises, d'assister les services d'urgence, etc. Comme données qui seraient géoréférencées, on a nommé le numéro postal d'acheminement, le lieu, l'emplacement des bureaux de poste avec rue et numéro de maison. On n'a jamais parlé à l'époque d'un traitement de données se rapportant à des personnes.

En automne 1998, nous avons appris que le but du projet, qui a entre-temps été rebaptisé «GEO-POST», est en passe d'être élargi. Il semble en outre que du personnel de la Poste a été mandaté pour rassembler des informations concernant les bâtiments et les appartements.

Des informations offertes par la Poste sur Internet font même de la publicité pour une connexion entre la base de données et les adresses de clients (par ex. à des fins de marketing). Un tel traitement ne peut se faire sans l'assentiment des personnes concernées. Nous sommes intervenus auprès de la Poste et avons demandé des informations complémentaires.

Dans notre 5e rapport d'activités (page 207) nous avons pris position sur le principe des risques concernant la protection des données liés aux données géocodées.

3.5. Communication par la Poste des noms des détenteurs de cases postales

Si quelqu'un désire connaître le détenteur d'une case postale, il doit rendre vraisemblable envers la Poste un intérêt légitime. La simple curiosité ne suffit pas. D'autre part,

une case postale n'est pas non plus faite pour couvrir les activités illégales de son détenteur.

Nous recevons occasionnellement des demandes concernant la communication de l'identité d'un détenteur de case postale, soit de la part de personnes qui entendent se défendre contre une personne ou une société dont il ne connaisse que l'adresse de la case postale, soit de détenteurs de cases postales qui désirent protéger leur sphère privée.

Conformément aux conditions générales de la Poste sur l'utilisation d'une case postale, le nom et l'adresse d'un détenteur de case postale ne peut être communiqué que si l'on peut rendre vraisemblable un intérêt légitime. La simple curiosité ou un envoi publicitaire isolé qui est ressenti comme harcèlement ne suffit pas. Les cases postales n'ont pas non plus été créées pour assurer un anonymat total à son détenteur. Il n'est pas prévu que l'existence de cette case le protège s'il exerce des activités peu sérieuses ou même illégales. A titre d'exemple, l'existence d'une créance non réglée constitue un intérêt légitime de la part d'un créancier.

Il faut reconnaître que l'appréciation peut ne pas toujours être facile. La Poste nous a pourtant assuré qu'elle était très exigeante en ce qui concerne l'établissement de la vraisemblance et qu'elle examinait sérieusement les demandes.

4. Internet et technologies de la vie privée

4.1. Conception et avantages d'un site Internet conforme à la protection des données

La mise en place d'une politique de traitement des données favorable aux principes légaux de la protection des données est une démarche payante. La confiance des utilisateurs s'en trouve accrue, ce qui se traduit ensuite par une plus grande fidélité de la clientèle et, généralement, par un élargissement de cette même clientèle. Ainsi, une étude menée aux Etats-Unis montre que la protection de la sphère privée est un argument majeur pour les prestataires de services en ligne désirant s'attacher de nouveaux clients.

Les consommateurs et utilisateurs de prestations en ligne ne sont pas toujours conscients de la quantité des informations traitées. Leurs centres d'intérêt sont

déterminés sur la base de leurs visites sur les sites Internet. Ces informations peuvent ensuite être vendues à des tiers. Bon nombre d'utilisateurs refusent donc d'introduire dans le réseau des informations les concernant. En effet, les prestataires ne sont pas à même de donner une réponse convaincante sur le but de la collecte d'informations ou sur leur future utilisation.

Seul un petit nombre de sites donnent des indications précises sur la protection de la personnalité ou indiquent l'utilisation qui sera faite des données personnelles ainsi rassemblées.

Nous recommandons donc aux exploitants de réseaux de développer une politique en faveur de la protection de la personnalité afin de répondre aux exigences légales (transparence, information, possibilité de choix, sécurité, consentement de la personne concernée). Cette politique leur permettra du reste de mettre en confiance leurs clients et les futurs utilisateurs.

Les principales mesures à prendre sont les suivantes:
- signaler en un endroit bien visible de l'offre à quelles dispositions légales de protection des données cette offre est soumise. En outre, la pratique du site en la matière doit être présentée dans un langage clair. Il convient en particulier de dire quelles données vont être relevées et utilisées, et dans quel but.
- Donner à l'utilisateur la possibilité de limiter cette utilisation (par ex. s'il s'oppose à l'élaboration de son profil de consommation) et la transmission des données le concernant (par ex. à des fins publicitaires).
- Selon la destination des données, prendre des mesures de sécurité garantissant l'exactitude, l'intégralité et l'actualité des données (par ex. méthodes de chiffrement et d'authentification).
- Enfin, mentionner la manière dont l'utilisateur peut faire valoir ses droits.

Certains traitements de données concernant les utilisateurs d'Internet sont susceptibles de contrevenir aux dispositions légales de protection des données. Pour cette raison, si l'utilisateur n'est pas informé au préalable, aucune donnée personnelle ne devrait être relevée, transmise à des tiers ou rendue accessible. (A ce propos et pour de plus amples informations très utiles, cf. p. 360 Lignes directrices du Conseil de l'Europe pour la protection des personnes à l’égard de la collecte et du traitement des données à caractère personnel dans les inforoutes ainsi que p. 364 Recommandations du rapport d’experts pour l'application de directives de l'OCDE sur la protection de la sphère privée dans les réseaux globaux)

4.2. Recommandations en vue de la protection de la sphère privée des utilisateurs d'Internet

Internet est une réalité de plus en plus présente. La période d'euphorie et d'émerveillement est passée. On ne voue même plus le «net» aux gémonies. C'est désormais un fait accepté par la politique et par la société. Aujourd'hui, la demande va plutôt dans le sens d'un usage rationnel d'Internet. En d'autres termes, on voudrait profiter des possibilités qu'offre le réseau, tout en luttant contre les risques, notamment les atteintes à la personnalité.

Internet permet d'accéder au niveau de la planète à des informations ou à des prestations. En même temps qu'ils surfent sur le net, les utilisateurs (souvent à leur insu) fournissent des données qui sont traitées, rassemblées, exploitées ou transmises à des tiers de diverses manières. Or les lois nationales sur la protection des données ne sont applicables que sur le territoire de l'Etat concerné. Pour cette raison, en cas d'atteinte à la personnalité, il est très difficile pour les personnes concernées de faire valoir leurs droits. Il n'existe actuellement aucune convention internationale qui protégerait efficacement la sphère privée sur Internet. Les utilisateurs de services Internet devraient donc être particulièrement prudents avant de permettre l'accès à leurs données personnelles.

Nous avons rassemblé ci-dessous quelques conseils permettant de mieux protéger la sphère privée sur Internet :

- sachez qu'en utilisant Internet, vos données personnelles sont relevées et enregistrées, en partie à votre insu.
- Assurez-vous d'abord que le traitement de données personnelles sur un site particulier est soumis à des dispositions précises de protection des données. Certains prestataires indiquent dans quel but les données sont relevées et quelle sera leur utilisation.
- Utilisez la dernière version des programmes de navigation qui offrent en général une meilleure sécurité.
- Protégez vos données (chiffrement, signature digitale), si vous voulez garantir leur intégralité et leur confidentialité. Vous pouvez charger gratuitement via Internet des logiciels qui permettent de chiffrer les données de manière sûre.
- Si vous participez à des groupes de discussion et acceptez de figurer sur des listes de participants, pensez que vos données, notamment votre adresse électronique (cf. également à ce sujet p. 299 sur la publicité par courrier électronique) sera enregistrée pour longtemps et accessible à tous. Vos données peuvent être réutilisées ou abusivement utilisées. Afin d'éviter cela, nous vous recommandons de faire usage des outils d'anonymisation gratuitement disponibles sur Internet.

- Ne réglez aucune affaire via Internet si la structure n'est pas dotée d'un système de sécurité.

Enfin, soyez toujours conscients que lorsque vous visitez les sites, vos destinations de prédilection seront pour la plupart enregistrées. Afin de l'éviter, fuyez les offres qui ne garantissent pas l'anonymat ou utilisez sinon les outils d'anonymisation.

A ce propos et pour de plus amples informations, se reporter p. 360 Lignes directrices du Conseil de l'Europe pour la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel dans les info-routes, p. 364 Recommandations du rapport d'experts pour l'application des directives de l'OCDE sur la protection de la sphère privée dans les réseaux globaux et thème suivant 4.3. sur l'utilisation de technologies respectant la protection des données.

4.3. Protection de la sphère privée grâce aux technologies favorables à la protection des données (technologies de la vie privée)

La multiplication des nouvelles technologies s'est traduite par une intensification du traitement des données. Grâce aux services en ligne, c'est désormais au niveau mondial que l'on échange, sauvegarde ou utilise même à d'autres fins des données personnelles, parfois à l'insu des personnes concernées. Grâce à la possibilité de traiter ces données personnelles à l'échelle de la planète et en l'espace de quelques secondes, il est de plus en plus difficile – si ce n'est impossible – pour les personnes concernées de protéger leur sphère privée ou de faire valoir leurs droits à temps. Elles sont donc invitées à faire preuve d'un plus grand sens de la responsabilité et à agir avec la réserve qui s'impose lorsque leurs données personnelles sont en jeu. Pour qu'elles puissent protéger elles-mêmes et directement leurs intérêts, il faut instituer et développer des technologies de la vie privée.

Internet, comme d'autres services en ligne, se caractérise entre autres par sa capacité à générer la transmission de très grandes quantités d'informations. L'accès des utilisateurs aux services en ligne est très rarement anonyme. En outre, la plupart des utilisateurs ignorent les risques que cette activité en ligne comporte pour leur sphère privée qui n'en est que plus menacée. Il convient donc de prendre des mesures qui limitent au minimum le relevé de données personnelles. Pour ce qui est de la protection de la sphère privée à l'aide de

moyens techniques – dans la mesure de ce qui est réalisable -, les services en ligne doivent tenir compte du besoin légitime d'anonymat. En effet, à l'ère des réseaux mondiaux, les lois sur la protection des données ne suffisent plus à elles seules à protéger le droit à la vie privée. La technique doit donc être utilisée de manière à ce que les systèmes de traitement de données permettent de limiter d'emblée au strict nécessaire le traitement de données personnelles.

Aujourd'hui déjà, il existe des moyens techniques favorables à la protection des données permettant de concevoir des systèmes qui ne nécessitent que peu de données ou qui garantissent l'anonymat (procédé de chiffrement, utilisation de pseudonymes dans des cas où l'identification de la personne n'est pas nécessaire, cartes à puces rechargeables, etc.). Néanmoins, dans la pratique, ces possibilités sont encore trop peu exploitées. Nous recommandons donc aux prestataires de services et aux fournisseurs de faire davantage usage de ces technologies compatibles avec la protection des données.

- Les systèmes de traitement de données en particulier doivent être conçus de manière à ce l'on relève aussi peu de données personnelles que possible.
- Les prestataires de services en ligne doivent, si la technique le permet, offrir des services anonymes aux utilisateurs. Un pas essentiel dans ce sens serait de fournir aux utilisateurs des moyens de paiement anonymes.
- Les prestataires de services devraient effacer les données personnelles qui ne sont plus nécessaires dans le cadre de la transaction avec l'utilisateur ou le consommateur.

Mais il est aussi dans l'intérêt des prestataires de services en ligne de promouvoir et d'offrir des technologies de la vie privée. Cela permet d'accroître la confiance des utilisateurs à l'égard de l'offre de prestations de services électroniques, confiance nécessaire pour que les prestations offertes rencontrent un écho favorable. La transposition du principe «protection des données par la technique» peut très bien être utilisée comme avantage sur la concurrence.

Enfin, il convient de ne limiter que dans la mesure du nécessaire par une loi et de manière permanente les restrictions au droit à l'anonymat ou les moyens techniques à cet effet (par exemple les procédés de chiffrement).

5. Commerce électronique et protection des données

5.1. Exigences minimales requises par la protection de la sphère privée dans le contexte du commerce électronique

La notion de commerce électronique englobe toutes les formes d'opérations électroniques liées à la vie économique. Autrefois, le commerce électronique se limitait princi-

palement au déroulement d'opérations à l'intérieur d'un groupe clos d'utilisateurs. Aujourd'hui, c'est une nouvelle forme, et non des moins importantes, des échanges économiques.

Le caractère global du commerce électronique implique une circulation intense de données personnelles qui, dans certains cas, est susceptible de porter atteinte à la sphère privée des personnes concernées. Il est donc essentiel que cette forme d'échanges économiques soit aussi soumise aux principes fondamentaux de la protection des données. La sécurité du droit est d'ailleurs un critère essentiel si l'on veut mettre les utilisateurs en confiance et s'assurer d'un bon accueil auprès du public. Un homme d'affaires ou un utilisateur n'aura recours aux possibilités offertes par ce marché mondial que si l'accès aux informations confidentielles est absolument fermé aux tiers. En effet, il sera d'autant plus enclin à faire appel à un service offert par voie électronique si ses données personnelles ne sont ni traitées, ni enregistrées contre sa volonté à d'autres fins (cf. Conférence d'Ottawa sur le commerce électronique, p. 345).

Chargé de concevoir un plan d'action pour le commerce électronique, l'Office fédéral des affaires économiques extérieures (OFAEE) nous a contactés. Nous lui avons signalé les mesures essentielles permettant la protection de la sphère privée dans le contexte du commerce électronique. Ces mesures ont été intégrées au plan d'action et portent sur les points suivants:

- sensibilisation des utilisateurs et des consommateurs sur les mesures indispensables à une protection efficace de la sphère privée dans le commerce électronique.
- Inventaire et contrôle des moyens techniques à mettre en œuvre dans le commerce électronique en vue de protéger la sphère privée.
- Face à la concurrence, tirer parti de la transposition technique de la protection des données (principe de la protection de la sphère privée par la technique) dans le domaine du commerce électronique.
- Etudier les effets de la législation actuelle en matière de protection des données sur la protection de la sphère privée dans le contexte du commerce électronique.

Nous avons complété ces mesures sur certains points à l'occasion d'un séminaire organisé par l'OFAEE sur le commerce électronique:

- les dispositions relatives à la protection de la sphère privée figurant dans la LPD sont à même d'accroître la confiance des utilisateurs à l'égard des prestations offertes par le commerce électronique.

- La LPD renferme des solutions flexibles pour le traitement de données personnelles par les personnes privées (art. 4 et 13 LPD) et est rédigée de manière neutre du point de vue technologique. Une révision immédiate de la loi ne s'impose donc pas.
- Néanmoins, les dispositions légales à elles seules ne suffisent pas à assurer la protection de la sphère privée des utilisateurs du commerce électronique. Il faut aussi et surtout les sensibiliser et les informer.
- A moyen terme, cette sensibilisation devra se faire par le biais de la formation continue et du perfectionnement professionnel.
- Les prestataires de services sont tenus de traiter de façon transparente les données relatives à leurs clients (comme le prévoit d'ailleurs la LPD) s'ils veulent accroître la confiance de ceux-ci à l'égard du commerce électronique. Ils sont tenus de leur indiquer sur quelles données personnelles porte le traitement et dans quel but ces données personnelles sont traitées. Si des données personnelles issues d'un rapport contractuel sont traitées dans un autre but (par ex. marketing, publicité), l'utilisateur doit avoir des possibilités de choix.
- Les techniques telles que les méthodes de chiffrement, d'identification ou autres procédés favorables à la protection des données comme les outils d'anonymisation garantissent la sécurité des données. Elles doivent être utilisées dans les échanges électroniques et mises à la disposition des utilisateurs.
- Enfin, la protection de la sphère privée, surtout la transparence du traitement des données, est à même d'accroître la confiance des utilisateurs à l'égard du commerce électronique. C'est là un aspect de la question que les entreprises suisses peuvent souligner comme avantage sur la concurrence.

6. Personnel

Administration fédérale

6.1. La communication de photos du personnel de l'administration fédérale

Le fait de considérer la diffusion de photos comme une communication de données personnelles dans un cas d'espèce ou par procédure d'appel dépend notamment du moyen de communication utilisé, ainsi que du cercle des destinataires. Alors que la publication dans un cas d'espèce est possible avec le consentement de la personne concernée, nous sommes parvenus à la conclusion qu'il faut renoncer à la diffusion de photos par procédure d'appel, par exemple sur Intranet. Indépendamment du critère de

la légalité qui n'est pas rempli, cette communication n'est pas utile à l'accomplissement des tâches légales de l'administration fédérale et peut révéler, dans certains cas, des données sensibles telles la race ou la religion des personnes concernées.

Certaines unités de l'administration fédérale ont pour habitude de publier la photo de leurs agents nouvellement engagés dans leur journal ou de l'envoyer à leur personnel par courrier électronique. Nous avons émis l'avis selon lequel ce type de communication, que l'on peut considérer comme une communication dans un cas d'espèce, est admissible avec le consentement de la personne concernée. Ces informations ne sont certes pas, sous l'angle de la proportionnalité, vraiment nécessaires à l'accomplissement des tâches légales de l'unité concernée, mais font partie de la culture d'entreprise, ayant notamment pour buts de faire connaître les nouveaux venus et de maintenir ainsi une certaine cohésion du personnel de l'organe concerné.

Des collaborateurs d'un office se sont en revanche opposés au projet de diffuser de manière systématique sur Intranet, outre des données personnelles les concernant, leur photographie. Or, le responsable de ce projet a refusé de tenir compte de l'opposition des intéressés. Nous avons dès lors contacté la direction de l'office pour la prier de faire bloquer la diffusion des photos, et de détruire les images déjà saisies pour les raisons suivantes. Une telle diffusion est une communication par procédure d'appel, qui, pour être licite, requiert une base légale. Pour qu'une telle base soit créée, encore faut-il que la nécessité de ladite communication soit reconnue. Or, ce n'est pas le cas en l'espèce, puisque sous l'angle de la proportionnalité, il est superflu de faire figurer les photos des agents d'un organe de l'administration sur Intranet, celles-ci n'étant pas nécessaires pour l'accomplissement des tâches légales de cet office, ni pour un agent d'un autre organe désireux d'entrer en contact avec ledit office.

Une telle diffusion implique également des risques pour la sécurité des personnes travaillant dans des domaines exposés. Ce danger ne doit pas être sous-estimé, car le caractère apparemment restreint du cercle de destinataires des informations d'Intranet est relatif. En effet, il n'y a pas que la Confédération qui, à notre connaissance, y a accès. D'autre part, la sécurité des données n'est pas garantie, et l'on ne peut pas exclure l'accès au réseau par des personnes non autorisées.

Finalement, une photographie, assimilable à un support d'informations, révèle non seulement des données personnelles, mais elle peut dans certains cas contenir des données sensibles telles la religion ou l'appartenance à une race.

6.2. Communication de sanctions disciplinaires accompagnée d'un exposé des motifs et de données relatives à la santé

L'admissibilité de la communication de sanctions disciplinaires, accompagnée des motifs et de données sur la santé, par un service juridique au service du personnel de la même unité administrative dépend de la portée du droit de regard du service du personnel en matière d'affaires disciplinaires. Ce droit de regard est différent selon les cas. En effet, au sein de l'administration fédérale, tous les services du personnel n'ont pas les mêmes attributions. Sans ce droit de regard, un service du personnel ne peut recevoir que le dispositif d'une décision.

Le chef du service juridique d'une unité de l'administration fédérale nous a demandé s'il était admissible que les sanctions disciplinaires rendues par le service juridique, y compris les motifs et des données sur la santé, soient remises au service du personnel de la même unité administrative. Nous lui avons donné la réponse suivante: le secret médical oblige le médecin à garder le secret sur les informations qui lui sont confiées dans le cadre de son activité professionnelle ou dont il a pris connaissance en exerçant cette activité. Les données sur les patients ne doivent être dévoilées à des tiers que si par exemple le patient libère le médecin de son devoir de discrétion ou si une loi l'y autorise. Les personnes dont la profession requiert la connaissance de données sensibles sont soumises au secret professionnel. Il y a atteinte au secret professionnel lorsque ces personnes communiquent sans y être autorisées des données sensibles. Ainsi, la transmission de données n'est pas autorisée lorsqu'elle est destinée à des personnes dont l'activité professionnelle ne nécessite pas la connaissance de données sensibles. Dans ce cas, la communication de données contrevient au principe de la finalité et de la proportionnalité. En outre, les organes de la Confédération ne sont en droit de traiter des données personnelles que s'il existe une base légale. On peut exceptionnellement communiquer des données personnelles sans base légale lorsque le destinataire a absolument besoin des données pour pouvoir accomplir une tâche clairement définie par la loi, lorsque la personne concernée y a, en l'espèce, consenti, ou que son consentement peut être clairement déduit des circonstances.
Dans le cas présent, il s'agit de savoir si le service du personnel est exceptionnellement autorisé à prendre connaissance des motifs de sanctions disciplinaires; en effet, ces motifs contiennent aussi des données sensibles sur la santé susceptibles de produire, prises dans leur ensemble, un profil de la personnalité bien qu'elles ne soient pas structurées. D'après nos recherches, il existe à ce propos différentes pratiques. Dans certaines unités administratives, les services du personnel n'ont pas seulement un droit de regard en matière disciplinaire, mais sont également habilités à rendre des décisions. Dans ce cas, c'est le

service du personnel qui rend les sanctions disciplinaires en faisant appel à des juristes. Il a alors le droit de consulter tous les documents qui sont à la base de la décision.
Puisque le droit de regard dépend des attributions de chaque service du personnel – lesquelles diffèrent selon les services dans l'administration fédérale –, nous avons proposé à la personne qui nous a consultés d'examiner avec le service du personnel de son unité administrative si celle-ci avait un droit de regard en matière disciplinaire. S'il avère que du fait de ses propres attributions, ce service ne bénéficie pas de ce droit, il ne pourra disposer, dans l'accomplissement de ses tâches administratives, que du dispositif de la décision.

6.3. Communication de données concernant les chômeurs aux autorités de poursuite pour dettes

Le Tribunal fédéral s'est exprimé sur la relation entre le devoir de discrétion des autorités de l'assurance-chômage et le devoir général de renseigner selon le droit sur la poursuite pour dettes et la faillite. Le jugement n'a pas rencontré l'écho attendu par les autorités en charge des assurances sociales.

Au début de l'année 1997, l'Office fédéral du développement économique et de l'emploi (OFDE) nous a prié de nous prononcer sur la relation entre l'obligation du secret posée par la loi sur l'assurance-chômage et le devoir général de renseigner posé par le droit sur la poursuite pour dettes et la faillite. Dans notre prise de position du 9 avril 1997 (cf. 5^{e} Rapport d'activités p. 125 et 272, ainsi que JAAC 1997 III p. 664 ss), nous sommes parvenus à la conclusion que la réglementation de la communication de données figurant dans la législation sur l'assurance-chômage doit être considérée comme «lex specialis» par rapport à la réglementation générale, non détaillée et contestée depuis sa mise en œuvre, de la communication de renseignements figurant dans le droit sur la poursuite pour dettes et la faillite. Dorénavant, la communication de données concernant les chômeurs aux autorités de poursuite pour dettes ne sera possible sans le consentement des assurés que si la loi sur l'assurance-chômage (LACI) le prévoit expressément. La loi sur la poursuite pour dettes et la faillite (LP) doit également être précisée dans ce sens. Le 24 mars 1998, le Tribunal fédéral a approuvé un recours de l'Office des poursuites de Zurich contre la décision du Tribunal administratif du canton de Zurich (ATF 124 III 170; cf. également le commentaire de M. Fey, dans «Aktuelle juristische Praxis», 10/98). Il motivait son arrêt essentiellement par le fait que le législateur suisse n'a pas exclu, ou seulement partiellement, les offices chargés des assurances sociales - notamment de l'assurance-chômage - , de l'obligation de renseigner vis-à-vis des

offices des poursuites. Quant à la question du rapport entre le devoir de renseigner conformément à la LP et le devoir de discrétion de la législation sur l'assurance-chômage, le Tribunal fédéral s'est toutefois contenté de renvoyer à la pratique antérieure selon laquelle le renseignement ne pouvait être refusé en invoquant le devoir de discrétion (art. 19, 1er al., lettre a LPD) si le débiteur lui-même est tenu de fournir les renseignements. Le Tribunal fédéral a motivé sa décision en se fondant également sur l'art. 19, 1er al., lettre a LPD selon lequel les organes fédéraux ne sont en droit de communiquer des données personnelles que si le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale. Ce faisant, il omet de voir cependant qu'il n'est plus exceptionnel que les autorités de poursuite pour dettes demandent des données aux autorités de l'assurance-chômage, mais que cette démarche est de plus en plus fréquente et systématique. Cette démarche nécessite des bases légales.
Du fait qu'en l'espèce, les traitements et communications de données étaient partiellement équivoques vus sous l'angle des dispositions de protection des données, nous avons contacté le Tribunal fédéral et lui avons demandé de prendre, en se fondant sur le droit de la poursuite pour dettes et la faillite, une ordonnance à propos du traitement de données personnelles par les autorités de poursuite pour dettes. Nous avons motivé notre requête d'une part sur le manque d'uniformité au niveau cantonal de la pratique de l'octroi des renseignements et d'autre part parce qu'une réglementation claire créerait la transparence et la sécurité du droit nécessaires pour les autorités et fonctionnaires concernés. Le Tribunal fédéral a rejeté notre requête en substance parce qu'il estimait qu'il n'y avait pas matière à agir. Le Tribunal fédéral a estimé pour le surplus qu'il ne pouvait éliminer les éventuelles contradictions entre la loi sur la poursuite pour dettes et la faillite d'une part et la loi sur la protection des données de l'autre.

Fin 1998, l'OFDE a émis une directive sur la réglementation de l'entraide administrative entre les autorités de contrôle des assurances et les offices des poursuites pour dettes à titre de complément à la réglementation du devoir de discrétion posé par le droit de l'assurance-chômage. La directive prévoit que les personnes qui participent à l'exécution, au contrôle ou à la surveillance de l'assurance renseignent sur demande et gratuitement les autorités de poursuite pour dettes lorsque celles-ci font valoir qu'elles ont besoin des renseignements en question pour pouvoir exercer les tâches qui leur sont imparties par la loi. Seules les autorités de poursuite pour dettes ont compétence pour calculer le minimum vital, le fixer ou encore le modifier, leurs décisions pouvant faire l'objet d'un recours selon les dispositions légales en matière de poursuites pour dettes. Les caisses de chômage ne peuvent donc modifier de leur propre initiative la quote-part saisissable ou le minimum vital calculé par les autorités de poursuite pour dettes, même pas dans le cadre d'un gain provisoire. En cas de saisie de l'indemnité journalière, on peut intervenir directement sur les prestations de l’assurance-chômage dépassant le minimum vital, les autorités de

poursuite pour dettes utilisent dans les dispositifs de leur décision au lieu d'un montant en chiffres une formulation comme «Les prestations de l'assurance-chômage qui dépassent le minimum vital de Fr. xx.- sont saisies». Ce système de saisie «ouvert vers le haut» permet de verser chaque mois aux autorités de poursuite pour dettes le maximum légal possible, à savoir la totalité des prestations de l'assurance-chômage – variables selon les mois – qui dépassent le minimum vital.

Après avoir rencontré une délégation de représentants des offices des poursuites, nous avons accepté cette solution comme réglementation intermédiaire. L'OFDE comme les autres organes chargés des assurances sociales réviseront la LACI dans le cadre de l'adaptation de la législation fédérale à l'art. 38 LPD.

6.4. Législation sur les fonctionnaires et BV-PLUS

Les exigences posées par la loi sur la protection des données à propos de la base légale requise pour le traitement des données concernant le personnel de la Confédération n'ont pas été suffisamment concrétisées par le projet de nouvelle loi sur le personnel de la Confédération.

Arrêté du Conseil fédéral relatif au nouveau système d'information du personnel de l'administration fédérale

Par arrêté du 19 décembre 1997, le Conseil fédéral a déclaré obligatoire l'utilisation du logiciel standard SAP R/3 HR pour le soutien informatique du secteur du personnel de l'administration générale de la Confédération. Selon cet arrêté, il est prévu de mettre en place un système central qui couvre les fonctions communes à tous les domaines ainsi que les besoins centraux. Les départements, groupements et offices peuvent utiliser individuellement les autres fonctions du logiciel standard. Le DFF a été chargé de mettre en place le nouveau système d'information du personnel. Sur la base de cet arrêté, nous avons prié le DFF de rendre une décision finale dans le sens de notre recommandation du 4 juillet 1996 (cf. 4^{e} Rapport d'activités, p. 125 et 271), à savoir que le traitement de données personnelles concernant le personnel de la Confédération n'ait lieu de manière centralisée que pour la gestion des salaires (cf. 4^{e} Rapport d'activités p. 171 ss). Le DFF nous a fait savoir que cette décision ne pourrait être prise qu'après l'analyse préalable, mais au plus tôt fin 1998. Cette analyse a été terminée fin octobre 1998.

La nouvelle loi sur le personnel de la Confédération

Après l'arrêté du Conseil fédéral, le DFF a entamé la procédure de consultation sur le projet de loi sur le personnel de la Confédération. Début décembre 1998, nous avons donc reçu ce projet. Ainsi que nous l'avions déjà constaté à plusieurs reprise à l'occasion de la procédure d'adaptation de la loi sur les fonctionnaires à la LPD, les nécessités de la LPD n'ont de nouveau pas été prises en compte dans le projet de loi sur le personnel de la Confédération. En particulier, ni le BV-PLUS, ni le traitement des données médicales concernant le personnel de la Confédération ne sont suffisamment ancrés dans la loi. Ainsi, les exigences exprimées par la Commission de gestion du Conseil national concernant la base légale n'ont pas été concrétisées. Nous n'avons donc pas pu nous rallier au projet de loi.

L'ordonnance sur la protection des données concernant le personnel de la Confédération

Après la prolongation de délai en vue d'adapter les bases légales requises à la LPD (voir aussi p. 318), le DFF a abandonné les travaux visant la création d'une ordonnance sur la protection des données concernant le personnel de la Confédération. Motifs: le Conseil fédéral aurait garanti par lettre du 27 avril 1998 de faire élaborer les bases légales pour la protection des données relatives au personnel de la Confédération, notamment les données relatives à la santé, dans le cadre de la révision totale de la loi sur les fonctionnaires, donc de la création de la nouvelle loi sur le personnel de la Confédération, et du remaniement de l'ordonnance sur le service médical de l'administration fédérale. Nous avons en outre informé le DFF que cette ordonnance doit être mise en place indépendamment de la création de bases légales formelles destinées à BV-PLUS, d'autant plus que les bases légales figurant dans la circulaire de l'Office fédéral du personnel du 26 janvier 1984 – c'est-à-dire les directives du Conseil fédéral du 16 mars 1981 – ont été abrogées. La circulaire de l'Office fédéral du personnel en date du 26 janvier 1984 sur la protection de données personnelles dans l'administration fédérale générale demeure en vigueur jusqu'à ce que l'ordonnance sur la protection des données concernant le personnel de la Confédération soit créée (voir notre site Internet www.edsb.ch).

6.5. Enregistrement des activités des utilisateurs accédant à Internet dans l'administration fédérale

La Conférence informatique de la Confédération de septembre 1998 a demandé au Préposé fédéral à la protection des données quelles étaient les conditions cadre du point de vue de la protection des données qui devaient être respectées lorsqu'on désire enregistrer les activités de personnes qui utilisent l'Internet.

Jusqu'à la remise de la demande citée ci-dessus, les collaborateurs de l'administration fédérale devaient signer un formulaire pour que l'accès à l'Internet leur soit accordé. Par leur signature, les utilisateurs acceptaient que leurs activités soient en majeure partie enregistrées dans un fichier de données situé dans le système pare-feu (firewall). Un tel enregistrement des activités sur Internet présente cependant le danger que l'on enregistre en même temps des profils de la personnalité des collaborateurs concernés. En outre, le risque existe également que les données enregistrées soient utilisées pour surveiller les collaborateurs (détournement de finalité).
Conformément à l'art. 17 al. 2 lit. c LPD, des profils de la personnalité peuvent être exceptionnellement traités dans les cas où les personnes concernées y ont, en l'espèce, consenti ou qu'elles ont rendu leurs données accessibles à tout un chacun. Il est cependant important de retenir que le consentement ne peut pas être donné de manière générale, mais qu'il est nécessaire séparément pour chaque cas. Si ni le caractère exceptionnel, ni le consentement de la personne concernée pour le cas précis, ni l'accessibilité publique des données existe, un traitement de profils de la personnalité ne peut avoir lieu que si une base légale sous forme d'une loi au sens formel existe (art. 17 al. 2 LPD). Avant de créer une base légale, il y a lieu d'étudier d'abord si le traitement de données personnelles est vraiment nécessaire pour l'accomplissement des tâches (principe de la proportionnalité). Dans le cas précis, il n'existe aujourd'hui aucune base légale. Il est cependant possible de mettre à disposition un instrument de contrôle conforme aux exigences de la protection des données sans base légale en procédant comme suit lors de la journalisation:
les adresses cible (URL) auxquelles les utilisateurs d'Internet de l'administration fédérale accèdent ainsi que les unités administratives (tels que offices et services) desquelles les demandes sont issues peuvent être enregistrés dans la mesure où il n'est pas possible d'identifier chaque utilisateur individuellement. Une telle journalisation serait conforme aux exigences de la protection des données puisque les offices ne sont pas des personnes morales et donc ne bénéficient pas de la protection de la LPD. En procédant à un dépouillement par échantillons des journaux, les cadres seraient en mesure de constater dans quelle mesure l'Internet est utilisé à des fins en rapport avec l'accomplissement des tâches.

Secteur privé

6.6. Dessinateur gaucher à la recherche d'un emploi

L'aptitude au dessin d'un candidat s'apprécie sur la base de critères qui n'ont aucun rapport avec la mention de «gaucher» ou «droitier». Cette mention porte néanmoins sur un état de fait qui peut avoir, selon les circonstances (situation financière ou taille de l'entreprise), une portée plus ou moins grande en vue de l'exécution du contrat de travail. Par exemple l'achat d'un appareil à dessiner pour gaucher sera éventuellement un investissement disproportionné. Dans ce cas, la question «gaucher» ou «droitier» peut se justifier.

Un dessinateur gaucher nous a demandé s'il était admissible de faire figurer la question «gaucher» ou «droitier» sur certains formulaires de candidature. Nous sommes parvenus à la conclusion suivante: dans le cadre d'un rapport de travail, les parties au contrat sont soumises à un devoir d'information découlant du principe de la bonne foi, et ce dès avant la conclusion du contrat. L'employeur posera donc avant même de conclure le contrat de travail toutes les questions en rapport avec l'emploi, compte tenu du genre de l'entreprise ainsi que de l'activité et de la position du candidat. De son côté, le candidat exercera son droit de la personnalité et protégera les faits touchant sa sphère privée – par exemple le fait qu'il travaille de la main gauche.
Le critère permettant de peser les intérêts des deux parties est en rapport avec l'emploi en question. En d'autres termes, les seules questions autorisées sont celles qui concernent l'aptitude du candidat à occuper le poste ou d'autres faits importants en vue de la concrétisation du contrat de travail. Pour savoir dans quelle mesure les questions relevant de la sphère privée du candidat présentent un rapport avec l'emploi en question, il convient d'examiner avant tout le genre de rapport de travail, la position du candidat ainsi que la taille et le domaine d'activités de l'entreprise. Le candidat ne doit pas répondre conformément à la vérité aux questions qui ne sont pas admissibles (droit de «légitime mensonge»). Exceptionnellement seulement, en cas de restrictions de la capacité de travailler du candidat – restrictions auxquelles l'employeur ne s'attend pas et qui empêchent dans la pratique l'exécution du contrat de travail – , le candidat est tenu de communiquer de lui-même ces faits sans y avoir été invité.

Nous avons communiqué aux personnes concernées notre avis à propos du rapport entre la mention «gaucher» ou «droitier» et le poste proposé: on juge l'aptitude d'un candidat au dessin d'après des critères qui n'ont rien à voir avec les mentions «gaucher» ou «droitier». Cette mention concerne néanmoins un

état de fait pouvant être plus ou moins important pour l'exécution du contrat de travail selon les circonstances concrètes (situation financière ou taille de l'entreprise). Ainsi on peut imaginer que l'engagement d'un gaucher implique pour une entreprise un investissement supplémentaire (par exemple l'achat d'un appareil à dessiner pour gaucher) démesurément élevé compte tenu de l'ensemble des circonstances (notamment la situation financière ou la taille de l'entreprise). Si tel est le cas, au moment où il s'agit d'apprécier les intérêts en jeu, les intérêts financiers de l'entreprise prévalent sur les intérêts du candidat à être employé par cette entreprise. La question «gaucher» ou «droitier» est donc justifiée dans ce cas et peut être posée au cours de la procédure de candidature. Il en va autrement lorsque du fait de la taille de l'entreprise et de sa capacité financière, l'acquisition d'un appareil à dessiner pour gaucher semble raisonnable. Dans ce cas, la question «gaucher» ou «droitier» n'est pas justifiée, ou ne l'est que pour des motifs d'organisation (par exemple quel bureau le nouveau collaborateur gaucher occupera-t-il). Le candidat ne devrait toutefois pas faire usage du droit de «légitime mensonge» dans le cadre de la procédure de candidature car il sera probablement dans l'incapacité de déterminer d'emblée la situation de l'entreprise (finances, taille). Il n'est toutefois pas soumis au devoir de communication quant à la mention «gaucher» ou «droitier». Il incombe par contre à l'entreprise de porter à sa connaissance les conditions d'engagement.

6.7. Conventions collectives de travail et protection des données

Le contrôle des livres de payes tels qu'il est prévu dans les conventions collectives de travail (CCT) a pour but la protection de la personnalité d'une multitude de travailleurs. De ce fait, les employeurs ne peuvent invoquer la protection des données pour refuser de remettre les documents utiles au contrôle.

L'organe de contrôle mandaté par les parties à la CCT procède, entre autres, au contrôle des livres de paye auprès des entreprises signataires. C'est à ce propos qu'a surgi la question de l'admissibilité, du but et de la proportionnalité de la collecte des données concernant les salaires.
Les CCT sont des contrats de droit privé passées entre les associations patronales et les organisations syndicales. Le contrôle des livres de paye, qui a pour but de vérifier le respect des CCT, est du ressort d'un organe constitué par la CCT. Cet organe traite les données concernant les parties au contrat. Pour bénéficier de la capacité contractuelle, les entreprises signataires doivent pouvoir être contrôlées. En d'autres termes, elles doivent tenir les livres de manière à ce que l'on puisse en tout temps vérifier que les dispositions de la CCT portant sur les salaires sont respectées. A cet effet, les entreprises soumises au contrôle

présentent entre autres les documents suivants: registres du personnel, feuilles de paye, rapports de travail, comptabilité.
Voici quelle a été notre conclusion à ce propos: le contrôle des livres de paye a pour objectif de vérifier que les parties au contrat respectent les dispositions de protection des salaires. Il permet donc de vérifier que les droits de la personnalité des travailleurs sont protégés. Les intérêts relatifs à la protection de la personnalité d'une multitude de travailleurs priment sur ceux d'une entreprise à maintenir secrètes les données concernant sa gestion des salaires. La présence d'un intérêt prépondérant pour la communication de ces données supprime la nécessité de requérir le consentement des travailleurs et son ancrage dans la CCT. La liste des documents requis par la CCT permet de contrôler efficacement les livres de paye. Elle est en outre adaptée au but poursuivi et proportionnelle. La communication de données doit néanmoins se limiter aux données des travailleurs, ceux-ci devant en être informés. On ne peut néanmoins justifier la communication de données à des tiers (débiteurs, créditeurs, clients, ...) tel que le permettrait la publication de la comptabilité concernant le personnel.

6.8. Projets «sans drogues» et protection des données

Dans le cadre des projets «sans drogues», l'employeur n'est habilité à traiter aucune autre donnée sur la santé que la mention «toxicomane» ou «non toxicomane». Au cas où il aurait l'intention de contrôler (screening de drogues, prélèvement d'urine) l'observation des règles convenues, les employés concernés doivent être expressément informés du caractère facultatif des contrôles.

Dans le cadre d'un projet «sans drogues» destiné aux apprentis, une entreprise a utilisé un formulaire «Examen médical d'aptitude pour les apprentis» comportant des questions sur les domaines les plus intimes de la vie privée et de la santé des apprentis. Selon le projet, l'apprenti se serait engagé par sa signature à se soumettre avant et pendant l'apprentissage à des contrôles faits au hasard (tests, prélèvement d'urine). En signant, il aurait en outre délivré le médecin du secret médical vis-à-vis de l'entreprise.
Nous sommes intervenus auprès de l'entreprise et l'avons informée que l'employeur ne devait traiter à propos de l'employé que les données concernant l'aptitude de ce dernier à occuper l'emploi en question ou à remplir le contrat de travail. Nous avons précisé que le respect de ce principe était d'autant plus important que les données personnelles – par exemple celles relatives à la santé – étaient sensibles. Le formulaire soumis à notre examen ainsi que la procuration à signer par l'apprenti délivrant le médecin du secret médical ne tenaient

aucunement compte des principes mentionnés ci-dessus. Ce qui était d'autant plus choquant que l'entreprise proposait essentiellement des places d'apprentissage en mécanique. Les questions sur la santé figurant dans le formulaire sont inutiles à la concrétisation de ce genre de rapports de travail.
La procuration figurant dans le même formulaire et autorisant la levée du secret médical constituait également une atteinte à la personnalité de l'apprenti car, au vu de la situation de l'emploi, la participation à un projet «sans drogues» n'est pas un acte volontaire. La seule chose admise serait un examen de santé établi par le médecin de la personne concernée dans la mesure où il se limiterait aux maladies déterminantes pour l'exercice de l'apprentissage entrant concrètement en question (par ex. allergies). Dans ce cas, le médecin ne communiquerait toutefois à l'employeur que la conclusion «apte» ou «inapte». Les autres informations sur la santé du candidat à propos de son aptitude à occuper un emploi déterminé sont soumises au secret médical et ne doivent être communiquées qu'avec le consentement exprès de la personne concernée.

L'entreprise a donc modifié son questionnaire en conformité avec la protection des données. Elle a en outre apporté à la procuration des changements selon lesquels les médecins ne devaient plus communiquer à l'entreprise que le résultat de l'examen médical. Néanmoins, nous avions encore des doutes quant à la nécessité de cette procuration et à la déclaration d'aptitude du médecin. Nous avons donc encore informé l'entreprise de ceci: le consentement des personnes concernées à ce genre de tests ne suffit que s'il est libre et repose sur une information claire. Comme la précédente, la nouvelle procuration ne constituait pas une libre déclaration de volonté de la part des apprentis concernés. En effet, étant donné la situation actuelle sur le marché de l'emploi, un apprenti ne peut se permettre de refuser une place d'apprentissage. Bien qu'une entreprise soit fondamentalement tenue de prendre des mesures pour offrir à ses collaborateurs et à ses apprentis les meilleures conditions de travail, on ne trouve dans la législation aucune base autorisant l'employeur à prendre des mesures préventives de lutte contre la consommation de drogues, c’est-à-dire préalables à la constatation de faits marquants (par ex. modifications du comportement, baisse du rendement, comportement agressif, consommation ouverte de drogues). Outre le fait qu'elle enfreint la législation, la nouvelle procuration constitue aussi une preuve de méfiance envers les apprentis (surtout à l'égard de ceux qui ne se droguent pas).
Nous avons donc proposé de concevoir ainsi le projet d'apprentissage «sans drogues»: l'employeur peut prendre des mesures en conformité avec le droit du travail, par exemple discuter avec l'apprenti, poser des conditions à la poursuite de la formation, si nécessaire faire appel à un service de consultation, dans le pire des cas prononcer un congé. Si l'employeur envisage de contrôler le respect du projet «sans drogues» par un screening ou une analyse d'urine, il faut que les personnes concernées soient expressément informées du caractère facultatif de

ces tests. Il convient de protéger les droits de la personnalité de l'apprenti toxicomane ou susceptible de le devenir en veillant à ce que les résultats concernant sa consommation de drogue et les mesures adoptées ne soient rendues publiques ni à l'intérieur, ni à l'extérieur de l'entreprise (sauf si les intérêts des autres travailleurs, par exemple leur santé, ou d'autres intérêts prépondérants l'exigent). L'entreprise est tenue d'appliquer strictement le secret professionnel notamment à l'égard de tiers. Les données personnelles traitées par l'employeur concernant son employé ne doivent être communiquées à des tierces personnes qu'avec le consentement exprès de l'employé, surtout lorsqu'il s'agit de données sensibles sur la santé. La communication de données relatives à la toxicomanie peut avoir de graves conséquences sur la réinsertion de la personne dans le monde du travail. Si cette personne devait subir un préjudice économique du fait de la communication non autorisée de données (si par exemple elle ne peut plus trouver d'emploi), elle peut faire valoir des prétentions touchant le droit du travail, les droits de la personnalité et les dommages-intérêts. L'employeur n'est tenu de fournir des renseignements à un nouvel employeur potentiel que si l'occupation du poste requiert absolument les informations sur la toxicomanie du collaborateur. La personne concernée devrait alors en être informée en priorité.

L'employeur n'est également pas en droit de faire appel lui-même et sans le consentement de l'apprenti concerné à l'autorité de surveillance ou à un service autorisé de traitement ou d'assistance. Si l'employeur ne sait plus que faire, il informera l'apprenti de l'existence de services spécialisés. L'employeur est autorisé à prévenir les parents si des intérêts prépondérants de l’apprenti ne s'y opposent pas. La répression pénale en relation avec l'abus de stupéfiants est du ressort des autorités compétentes. L'employeur n'est en aucune manière tenu de dénoncer le cas. Il ne doit pas y avoir de surveillance systématique du comportement des collaborateurs et des apprentis. Le maître d'apprentissage ne doit donc pas surveiller activement l'apprenti pour voir s'il se drogue.

L'entreprise nous a garanti que les principes de protection des données seraient respectés. Elle a fait remplacer le formulaire «Examen médical d'aptitude pour les apprentis» par un formulaire en conformité avec la protection des données et établi une lettre d'information sur le caractère volontaire du test à l'intention des apprentis concernés et de leurs parents.

7. Assurances

Assurances sociales

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

En vertu de la loi sur la protection des données, les fichiers contenant des données sensibles ou des profils de la personnalité ne devraient pouvoir être traités que si une loi au sens formel l'autorise de manière explicite. Les bases légales requises doivent être établies au 31 décembre 2000. Or un retard important a été accumulé à cet égard, notamment dans le secteur des assurances sociales.

La LPD prévoit qu'au plus tard 5 ans après l'entrée en vigueur de ladite loi, les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité ne pourront être traités que si une loi au sens formel le prévoit expressément. Ce délai est échu au 1er juillet 1998.
Il était néanmoins prévisible, dans bien des domaines, que ce délai ne pourrait être tenu. C'est notamment le cas de la législation sur les assurances sociales. Le directeur de l'Office fédéral des assurances sociales (OFAS) a donc demandé à la Commission des affaires juridiques du Conseil des Etats de prolonger ce délai de transition jusqu'au 31 décembre 2000. Le Conseil fédéral également a prié la même commission de repousser ce délai non pas jusqu'au 30 juin 1999 comme il avait été prévu, mais jusqu'à la fin 2000. Le Conseil fédéral a demandé en outre aux offices d'établir un inventaire ainsi qu'un plan de réalisation des travaux législatifs requis (cf. 5e Rapport d'activités, p. 218 ss). Cette prolongation jusqu'à la fin de l'an 2000 est enfin entrée en vigueur par arrêté fédéral du 26 juin 1998.
L'OFAS a entre temps présenté plusieurs avant-projets au PFPD, qui a relevé à leur propos un certain nombre de points. Tout d'abord, le but du traitement des données doit être défini aussi clairement que possible dans la loi. En outre, la transmission de données (exceptions au secret professionnel) nécessite une base légale au sens formel pour toutes les données touchant aux assurances sociales; c'est à plus forte raison le cas lorsque ces données sont destinées à être transmises à des tiers dans un autre but. Par exemple la transmission de données relatives à l'AVS aux autorités fiscales dispose aujourd'hui déjà d'une base dans la loi sur l'AVS. Il est enfin nécessaire de répertorier les éventuelles possibilités de consultation des fichiers par procédure d'appel. En effet, s'il permet d'accéder à des données sensibles ou à des profils de la personnalité, ce mode de consultation doit aussi être réglé par une loi au sens formel. En matière d'AVS

par exemple, il convient notamment d'examiner si la Centrale de compensation donne la possibilité d'accéder à des données personnelles par procédure d'appel. L'OFAS élabore actuellement un projet de loi dans ce sens.

7.2. Avoirs «oubliés» des caisses de pension

Quelques caisses de pension retiennent des avoirs qui, jusqu'à ce jour, n'ont pas été versés à leurs ayants droit. L'Office fédéral des assurances sociales entend à ce propos mettre sur pied un service central chargé du 2^{e} pilier qui aura pour tâche de retrouver les adresses des ayants droit. Le préposé fédéral à la protection des données s'est exprimé de manière fondamentalement positive sur ce projet.

Les communiqués de presse font état d'au moins 420 millions de francs correspondant aux avoirs oubliés déposés dans le cadre du 2e pilier sur environ 70'000 comptes en Suisse. Il s'agit probablement dans la plupart des cas de 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. Ce fait a donné lieu à diverses interventions politiques et diplomatiques.
Le Conseil fédéral estime que la Suisse et les caisses de pension ont un devoir d'assistance envers les assurés. Il a donc proposé une révision de la loi sur le libre passage. Il s'agit notamment d'obliger les organismes de prévoyance à annoncer les avoirs oubliés auprès des caisses de pension à la future Centrale du 2e Pilier. Celle-ci recherchera les adresses des ayants droit dans le registre des rentes de l'AVS, en collaboration avec la Centrale de compensation. Par ailleurs, les assurés seront eux aussi tenus de fournir à la centrale les informations nécessaires pour que celle-ci puisse faire ses recherches.
Dans le cadre de la consultation des offices, nous avons rendu un avis fondamentalement positif sur le projet. Le principe de la proportionnalité y est particulièrement respecté. Nous avons également souligné la nécessité de trouver le plus rapidement possible une solution à ce problème dans l'intérêt des ayants droits.

7.3. Sélection illégale des risques dans le domaine de l'assurance-maladie obligatoire

Les pratiques en matière d'admission qui ont pour but la sélection des risques dans l'assurance de base obligatoire contreviennent aux lois sur l'assurance-maladie et sur la

protection des données. Néanmoins, le risque d'abus demeure tant que les assureurs continuent à avoir accès à des données concernant l'âge et l'état de santé. Le préposé fédéral à la protection des données s'est prononcé pour deux différents formulaires d'adhésion: l'un pour une assurance de base (sans question sur l'état de santé), l'autre pour l'assurance complémentaire.

Les questions sur l'état de santé qu'un assureur pose dans le formulaire de demande d'adhésion à l'assurance-maladie obligatoire contreviennent à l'esprit et à la lettre de la loi fédérale sur l'assurance-maladie (LAMal). Cette loi prévoit entre autres l'obligation d'être assuré ainsi que le libre choix de la caisse-maladie. Nul n'ignore que toutes les caisses-maladie sont obligées d'accepter les personnes qui demandent à être admises pour l'assurance de base, indépendamment de leur état de santé. Les caisses sont également dans l'impossibilité de subordonner les modifications de franchise à l'état de santé des individus (cf. également la circulaire 97/9 du 12 novembre 1997 de l'Office fédéral des assurances sociales).
Si elles concernent l'assurance de base, les questions portant sur l'état de santé d'une personne qui désire changer de caisse contreviennent aussi aux dispositions de protection des données. En vertu de l'obligation d'être assuré, il n'est ni requis, ni approprié de demander des renseignements concernant la santé d'un individu (atteinte au principe de la proportionnalité en vertu de l'art. 4, 2e al. LPD). En outre, il manque la base légale formelle qui autoriserait les caisses-maladie à requérir des données relatives à l'état de santé de la personne en question en vue de l'assurance-maladie obligatoire.
Par contre, s'il s'agit de l'assurance complémentaire, il est permis de poser des questions sur l’état de santé. Mais seules les questions véritablement nécessaires et appropriées sont admises.
Une enquête menée par le PFPD auprès des assurances-maladie a révélé que la plupart des formulaires de demande n'indiquent pas clairement qu'en cas de changement d'assurance-maladie obligatoire, le relevé de données sur l'état de santé n'est pas permis. Certaines caisses-maladie ont laissé traîner les dossiers de demande d'adhésion émanant d'assurés déjà âgés et malades, d’autres caisses les ont même totalement ignorés. Afin d'éviter ce genre d'abus à l'avenir, nous avons demandé aux caisses-maladie d'établir des formulaires de demande distincts: l'un pour l'assurance de base (sans question sur l'état de santé), l'autre pour l'assurance complémentaire (avec les questions nécessaires sur l'état de santé).
Par ailleurs, les agents d'assurances qui essaient de recruter une clientèle essentiellement jeune et en bonne santé pour l'assurance de base contreviennent aussi à la loi sur la protection des données.

7.4. Analyse des procédures dans le domaine des assurances sociales

Nous avons constaté que l'organisation comme les structures internes dans le secteur des assurances sociales sont incompatibles avec les principes de la loi sur la protection des données. Nous avons donc l'intention d'analyser les procédures au sein des diverses autorités en charge des assurances sociales. Cette démarche simple permettra d'éliminer les atteintes à la protection des données dues au système.

Dans la pratique, nous sommes en général confrontés à des cas individuels. Lorsqu'il y a atteinte à la protection des données, de mauvaises structures internes au sein de l'organisation même en sont souvent la cause. Il arrive ainsi que des données soient transmises à des tiers bien que la loi l'interdise strictement. Par ailleurs, des données personnelles sont régulièrement échangées en très grandes quantités (violation du principe de la proportionnalité).
Citons un premier exemple: une caisse de compensation a transmis des données personnelles à une compagnie d'assurance privée. La caisse de compensation avait cru, à tort, que la compagnie en question était une assurance-maladie autorisée, qui avait fourni des prestations préalables dans l'affaire en question. Cependant, étant donné que la compagnie d'assurance n'était pas une caisse-maladie reconnue, elle n'était par conséquent pas autorisée à réclamer d'éventuelles prestations. La caisse de compensation a donc transmis illicitement à des tiers des données personnelles touchant le domaine protégé des assurances sociales.
Dans un autre cas, il s'agissait également de droits de prestations mutuels entre un service AI et une institution de prévoyance LPP, lequel service AI avait transmis inutilement l'ensemble du dossier à l'institution de prévoyance. A propos de ce cas, il est intéressant de noter que l'institution de prévoyance LPP offrait en plus un certain nombre d'assurances privées.
Dans le domaine de l'assurance-accidents, on a constaté dans bien des cas que l'accès aux renseignements demandés n'était pas du tout accordé ou seulement de manière lacunaire, là aussi souvent en raison d'un défaut d'organisation.
Ce ne sont là que quelques carences auxquelles une analyse des procédures permettrait de remédier. Nous estimons donc utile d'examiner à fond et de manière systématique les différentes structures internes. Cela demandera néanmoins énormément de temps. Il est prévu en 1999 de procéder tout d'abord à une analyse de ce type auprès d'un centre régional de placement, puis auprès d'un service chargé de l'AI.

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

Le 20 février 1998, le Conseil fédéral a créé la Commission d'experts sur la protection de la personnalité dans l'assurance-maladie et l'assurance-accidents sociales et privées. Les travaux de la commission sont en cours.

Cette commission a entre autres pour tâche de poursuivre les travaux du groupe de travail «Protection des données et listes des analyses / assurance-maladie» (ADAK I, Aspects de la sécurité sociale no 2/96, disponible auprès de l'OFAS). Elle est composée de représentants de diverses autorités et groupements d'intérêts concernés par l'assurance-maladie et l'assurance-accidents. Le PFPD y est également représenté.
La commission d'experts s'occupe tout particulièrement de la protection de la personnalité dans l'assurance-maladie et dans l'assurance-accidents sociales et privées. Les droits de la personnalité des individus concernés se heurtent souvent aux besoins d'informations des assureurs d'une part et à la politique en matière de santé de l'autre. La commission se penche actuellement sur les sujets suivants: quelle forme prendra le flux de données entre les prestataires de services et les assurances-maladie (code CIM-10, etc.)? Dans quelle mesure la fonction de médecin-conseil doit-elle être conservée ou modifiée dans le cadre de la LAMal? Est-il judicieux de créer une fonction similaire dans le domaine de l'assurance-accidents comme le PFPD et les ouvrages spécialisés le requièrent depuis des années déjà? Il lui faudra aussi examiner si et dans quelles conditions des données personnelles relevant de l'assurance de base obligatoire peuvent être transmises vers l'assurance complémentaire.
Enfin, une question très délicate se pose également: l'employeur peut-il consulter des données d'assurance et si oui, lesquelles. Cela concerne avant tout l'assurance LPP, mais aussi l'assurance d'indemnité journalière pour maladie que concluent les nouveaux employés. Il est courant à ce propos que l'employeur puisse consulter sans y être autorisé les données les plus sensibles concernant la santé de son employé, ce qui peut avoir des répercussions très négatives pour celui-ci.
La commission examinera bien d'autres questions encore. Les travaux de la commission sont en cours à l’heure actuelle.

7.6. La pratique de la communication des renseignements dans le domaine de l'assurance militaire

La communication des renseignements telle qu'elle est pratiquée dans le domaine de l'assurance militaire est incompatible avec la loi sur la protection des données. Le dépôt des dossiers pour consultation auprès des autorités communales pose à cet égard le problème majeur. Il est également irrecevable que l'Office fédéral de l'assurance militaire demande plus de Fr. 300.- pour des copies.

A plusieurs reprises, des particuliers ont attiré notre attention sur la pratique de l'Office fédéral de l'assurance militaire (OFAM) en matière de communication de renseignements. L'OFAM fonde sa pratique sur les dispositions de la loi fédérale sur la procédure administrative (PA), laquelle prévoit que les dossiers peuvent être consultés au siège de l'autorité de décision ou d'une autorité cantonale désignée par l'autorité de décision. En règle générale, les dossiers sont déposés pour consultation auprès de l'administration communale compétente. Si quelqu'un désire son dossier sous forme de copies, l'OFAM exige Fr. -.50 par copie.
Cette procédure ne doit pas être appliquée si elle contrevient à la LPD. En effet, la LPD est relativement récente et, en général, prime sur les textes légaux plus anciens. Ce principe s'applique également lorsque l'ancien texte n'a été ni abrogé, ni révisé formellement.
Les renseignements en vertu de la LPD sont en règle générale fournis gratuitement et par écrit, sous forme d'imprimés ou de photocopies. Il est possible de faire exception à cette règle de la gratuité lorsque la communication des renseignements demandés occasionne un volume de travail considérable. Néanmoins, on ne peut faire valoir un volume de travail considérable lorsque l'organisation et l'administration interne sont déficientes. Par ailleurs, le montant prélevé ne doit pas excéder Fr. 300.--.
Contrairement à la pratique de l'OFAM, les renseignements doivent être communiqués par écrit. Il n'est en aucun cas compatible avec la LPD que le dossier soit déposé pour consultation auprès d'une administration communale. D'une part il n'est ni indiqué, ni nécessaire que les employés des autorités communales aient également accès à des données sensibles touchant l'assurance militaire (violation du principe de la proportionnalité). D'autre part, il faudrait pour cela une base légale formelle (communication de données personnelles sensibles par l'OFAM à une autre autorité). En revanche, mais seulement si la personne concernée donne son accord, la consultation du dossier sur place est possible.
La pratique de l'OFAM consistant à demander d'une manière générale Fr. -.50 par copie contrevient également à la LPD. Il est déjà arrivé, lorsque les dossiers sont très volumineux, que l'OFAM demande plus de Fr. 300.- à la personne concernée.

Nous avons donc attiré l'attention de l'OFAM sur cette question et l'avons prié d'octroyer le droit d'accès au sens voulu par la LPD.

7.7. Cas concernant le domaine de l'AVS et de l'AI

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

Les centres de désintoxication reçoivent, à certaines conditions, des subventions AI de la part de l'Office fédéral des assurances sociale. Pour ce faire, ce dernier a besoin de données sensibles. Cependant, la collecte de données personnelles n'est autorisée que si les bases légales requises sont données. En outre, les personnes concernées doivent en être suffisamment informées.

Plusieurs centres de désintoxication ont demandé au PFPD si la pratique de l'Office fédéral des assurances sociales (OFAS) en matière de subvention était conforme à la protection des données. Un centre accueillant des personnes en désintoxication doit répondre à certaines conditions pour pouvoir bénéficier de subventions de l'AI. L'OFAS examine entre autres si les résidants présentent une atteinte à la santé à prendre en considération sous l'angle de l'AI. Pour pouvoir juger du cas, l'OFAS a besoin de données sur la santé de la personne concernée.
L'OFAS collecte donc des données sensibles (données sur la santé), ce qui requiert en principe une base légale au sens formel. A notre connaissance, l'OFAS fonde sa pratique en matière de subvention essentiellement sur la jurisprudence du Tribunal fédéral des assurances, ainsi que sur des directives internes.
Nous avons signalé à l'OFAS que ces bases légales sont à nos yeux insuffisantes. Par ailleurs, toute collecte de données doit être transparente En outre, s'il y a collecte systématique de données, l'OFAS est tenu de communiquer le but de la collecte, la base légale du traitement, les catégories des participants au fichier ainsi que des destinataires des données. Il a donc été convenu avec l'OFAS de remettre aux personnes concernées une notice les informant de manière suffisante du traitement envisagé. Enfin, nous lui avons fait observé que le nombre des questions devait être limité au minimum.

- Introduction d'un service médical dans le domaine de l'AI

Le préposé fédéral à la protection des données n'a rien à objecter à l'introduction d'un service médical dans le domaine de l'AI, à la condition cependant que ce service médical soit indépendant des autres autorités. En outre, ce service doit revêtir une fonction de «filtre». En d'autres termes, il ne communiquera à des tiers (par exemple les service AI) que les données personnelles effectivement nécessaires.

La révision de la loi sur l'assurance-invalidité (LAI) prévoit entre autres l'introduction d'un service médical. Le nouvel art. 53, 2e al. LAI sera ainsi libellé: «Le Conseil fédéral règle les modalités d'organisation du service médical et les tâches de ce dernier, ainsi que les compétences de l'Office fédéral.»
Les dispositions relatives à ce service médical ne nous ont pas été soumises lors la consultation des offices à propos du règlement sur l'assurance-invalidité (RAI). Nous avons néanmoins émis à cette occasion un certain nombre de remarques fondamentales sur l'institution du service médical dans le domaine de l'assurance-invalidité.
Le libellé prévu de l'art. 53, 2e al. LAI est insuffisant car le service médical traite des données personnelles. A notre avis, la LAI aurait dû définir avec précision au moins le but, l'organisation ainsi que les tâches de ce service médical. En effet, il traitera des données sensibles (données sur la santé), ce qui nécessite une réglementation claire et complète dans le cadre d'une loi au sens formel.
A notre avis, il est également important que le service médical en matière d'assurance-invalidité agisse comme «filtre indépendant».
Selon le principe de la proportionnalité, le traitement ne doit porter que sur les données personnelles appropriées et nécessaires pour atteindre le but poursuivi. Le service médical doit donc filtrer les informations et ne doit transmettre au service AI que les données nécessaires au cas traité.
L'indépendance du service médical est un élément permettant de garantir au maximum les droits de la personnalité des assurés. Il serait donc judicieux qu'il soit séparé des autres autorités, que ce soit du point de vue des locaux, de l'organisation et du personnel. Il faudrait en particulier éviter que les employés du service médical dépendent des autorités de décision. Enfin, nous avons également suggéré que le service médical soit surveillé par un organisme neutre et indépendant. Cette mesure réduirait le risque de voir le service médical réduit à un service chargé uniquement d'économiser les coûts.
Le référendum contre la révision de la loi sur l'assurance-invalidité a abouti. On ne sait donc pas à l'heure actuelle si le service médical sera introduit.

- Deux numéros d'assurés pour un certificat d'assurance AVS

La personne qui possède deux différents numéros d'AVS risque d'être exposée à des discriminations dans la vie quotidienne. C'est notamment le cas lorsque deux numéros, le «masculin» et le «féminin», figurent sur le certificat d'assurance.

Une personne s'est adressée à nous pour nous exposer son problème: elle a subi il y a quelques années une opération lui ayant permis de changer de sexe et d'adapter son organisme, à l'origine masculin, à son âme féminine. Ce qui s'était traduit depuis par l'inscription sur son certificat d'assurance AVS de deux numéros, le masculin et le féminin.
Cette personne, qui vit maintenant en tant que femme, demanda donc à sa caisse de compensation un certificat d'AVS comportant un seul numéro, le féminin. Elle fit valoir notamment que cet état de fait l'exposait dans la vie quotidienne à des situations de discrimination. Ainsi, s'étant présentée pour un nouvel emploi, elle s'était vue dans l'obligation de présenter à son futur chef du personnel un certificat d'assurance comportant deux différents numéros d'assuré. Elle s'était sentie atteinte dans sa personnalité et dans sa dignité humaine.
Malgré les préoccupations légitimes de cette personne, les autorités compétentes de l'AVS n'ont pas répondu positivement à sa requête. Au yeux des autorités, des raisons administratives s'y opposaient, notamment parce qu'il aurait fallu reconstituer l'ensemble des versements.
Le PFPD pria l'Office fédéral des assurances sociales (OFAS) de lui venir en aide. L'OFAS répondit aux vœux de cette femme et lui fit établir un nouveau certificat d'assurance avec un numéro d'AVS «féminin». La connexion avec l'ancien numéro d'assuré «masculin» a été assurée par l'OFAS au niveau interne.

- Le «registre-miroir» de l'AVS

Le «registre-miroir» de l'AVS doit être prochainement introduit. L'Office fédéral des assurances sociales s'est déclaré prêt à mettre en place la base légale requise. Néanmoins, le dépôt d'interventions parlementaires a retardé le projet.

Le «registre-miroir» de l'AVS a pour but de traiter plus rapidement les demandes que les personnes privées déposent auprès des caisses de compensation sur les cotisations qu'elles ont déjà versées. Il permettra aux caisses de compensation d'accéder plus rapidement aux comptes individuels (CI).
Le PFPD s'est exprimé positivement sur ce projet, à la condition que la protection des données et notamment la sécurité des données – dont le contrôle de l'accès – soient garanties (cf. 5e Rapport d'activités, p. 186 ss).

Les contributions des assurés sont répertoriées sur les CI. Ces comptes rassemblent entre autres les données suivantes: nom, no d'AVS, date de naissance, pays d'origine, numéro de décompte, code de revenu, durée de contribution (début/fin), année de contribution, revenu, employeur ou genre de revenu.
Les données figurant sur le CI sont à nos yeux susceptibles de constituer des profils de la personnalité au sens visé par la LPD. Ils permettent en tout cas de reconstituer toute une vie de travail, dont éventuellement et aussi les périodes de chômage. Ne serait-ce que les informations sur le salaire sont dans notre société un sujet très délicat.
A première vue, les CI ne peuvent contenir aucune donnée sensible. Pourtant, ce n'est pas toujours le cas. Par exemple les citoyens de nationalité israélienne qui paient leurs cotisations AVS sont probablement de religion juive. Si de telles données tombaient dans de mauvaises mains, cela pourrait avoir aujourd'hui encore des conséquences néfastes.
Du fait de la sensibilité des données personnelles traitées, nous demandons que le «registre-miroir» de l'AVS repose sur une base légale au sens formel, notamment parce que les données personnelles en question seront accessibles par procédure d'appel. La dimension de ce registre requiert aussi la création d'une base légale formelle. Par ailleurs, un fichier de ce genre réveille la «faim de données» ou l'intérêt de divers autres services. L'Office fédéral des assurances sociales (OFAS) a fini par se rendre à nos arguments et s'est déclaré prêt à préparer les bases légales nécessaires.
Le «registre-miroir» de l'AVS a également donné lieu à des interventions au niveau politique. En 1997, le conseiller national Hans Rudolf Gysin a déposé une interpellation ainsi qu'une motion. La motion du 10 octobre 1997 demandait au Conseil fédéral d'interdire le «registre-miroir» par une loi, en invoquant essentiellement le fait que la protection des données n'était plus garantie. L'OFAS a donc suspendu ses travaux et attend la décision du parlement sur le sujet.

- Splitting et divorce: vue d'ensemble des comptes AVS

Une caisse de compensation a livré à une femme un récapitulatif des versements AVS de son ex-mari. La remise de ce genre de document contrevient à la loi sur la protection des données lorsque les versements concernent la période qui a suivi le divorce.

Une femme nous a signalé qu'une caisse de compensation lui avait remis un récapitulatif du compte AVS de son ex-mari non seulement pour la période qui précédait le divorce, mais aussi pour celle qui le suivait. Estimant inutile de pouvoir consulter les données concernant le revenu de son ex-mari qui se référaient à la période après leur divorce, elle demanda à la caisse de compensation

de ne pas informer de même son ex-mari. Il n'y avait en définitive aucune raison, à son avis, que son ex-mari soit informé de sa situation financière consécutive au divorce. La caisse de compensation chargée du dossier refusa de répondre aux souhaits de cette femme.
Nous partageons entièrement l'avis de celle-ci et avons obtenu confirmation de l'Office fédéral des assurances sociales (OFAS). Seul le revenu des deux époux durant le mariage est déterminant en cas de divorce. Le revenu total durant le mariage est partagé, ce qui permet de déterminer les rentes AVS (splitting).
Les époux divorcés peuvent demander à la caisse de compensation d'établir les prétentions AVS découlant de l'union conjugale. Néanmoins, il est disproportionné de les informer de leurs conditions de revenus réciproques (employeur compris, etc.) après le divorce. A la suite de cela, l'OFAS est intervenu auprès de la caisse de compensation chargée du cas.

7.8. Principe de l'examen d'office et droits de la personnalité dans le domaine des assurances sociales

Dans le droit des assurances sociales, les autorités doivent établir les faits d'office, tout en étant néanmoins tenues de respecter les droits de la personnalité des assurés. Cette règle est particulièrement importante en matière d'assurances sociales où la plupart des données traitées sont sensibles.

Plusieurs personnes privées se sont adressées à nous pour savoir dans quelle mesure une assurance sociale était habilitée à enquêter sur les faits. Le domaine des assurances sociales est soumis au principe selon lequel l'autorité de décision est tenue d'office d'établir les faits pertinents ou de les constater, de sa propre initiative et indépendamment de la présentation de moyens de preuves des parties. Ce principe est néanmoins restreint par le devoir de participation selon lequel la personne qui déduit des droits d'une requête auprès de l'organisme d'assurance sociale ou qui est tenue de fournir des renseignements, doit participer à l'établissement des faits.
Il convient par ailleurs de respecter les droits de la personnalité des assurés. Selon eux, toute personne doit pouvoir rester maître des données la concernant et en limiter aussi le traitement. Plus les données sont sensibles, plus il convient d'y veiller.
Le problème majeur dans le domaine des assurances sociales et de l'assurance-accidents est le manque de transparence du traitement des données effectué par les assureurs. La personne assurée ne sait en général pas auprès de qui l'assurance a collecté des données, dans quel but et à qui elle les a communiquées. Le principe de la transparence est un principe figurant dans la LPD. La collecte de

données sensibles ou de profils de la personnalité des assurés notamment doit être effectuée de façon reconnaissable pour ces derniers (cf. art. 18, 2e al. LPD).
Nous constatons par ailleurs que les assurances sociales d'une part collectent trop de données et d'autre part en communiquent trop à des tiers (violation du principe de la proportionnalité). La personne qui rend vraisemblable un intérêt légitime peut exiger de l'assurance sociale (en l'espèce agissant comme organe fédéral) une décision susceptible de faire l'objet d'un recours. L'assuré peut notamment s'opposer à la communication de certaines données personnelles (art. 20 LPD). Celui qui s'oppose à la communication de données le concernant a le droit d'obtenir une décision. Si une telle communication a lieu, elle est tout simplement illicite.
Le principe de l'examen d'office et les droits de la personnalité doivent être pris en compte de manière équilibrée. Le libre choix de la personne concernée est un principe fondamental. Un traitement des données contre la volonté de l'assuré ne saurait être admis que si c'est le seul moyen d'établir les faits. Néanmoins, tant qu'il y a d'autres possibilités de déterminer les faits, la protection de la personnalité a la préséance.
Il manque actuellement les règles juridiques qui concrétiseraient les droits de la personnalité dans les divers textes de loi concernant les assurances sociales. Néanmoins, les principes de la protection de la personnalité sont d'ores et déjà applicables.

Assurances privées

7.9. Communication de données personnelles à l'étranger dans le domaine de l'assurance responsabilité civile

Les compagnies d'assurance-responsabilité civile font de plus en plus souvent établir leurs expertises à l'étranger. Néanmoins, dès qu'il y a communication de données personnelles à l'étranger, les prescriptions en matière de protection des données doivent être respectées.

Face à un sinistre, une assurance-responsabilité civile devra déterminer si elle couvre ou non un sinistre. Nous constatons à ce propos que de plus en plus d'expertises biomécaniques sont établies à l'étranger, et ce contre la volonté des personnes concernées. Les traumatismes de la nuque et de la colonne vertébrale notamment sont très fréquents en cas d'accidents de la circulation. Leur cause est très contestée dans les ouvrages spécialisés comme dans la jurisprudence. Une expertise biomécanique permet aux assurances-responsabilité civile de

savoir s'il y a ou non rapport de causalité entre l'accident et les douleurs dont souffre la personne concernée.
En général, l'expertise biomécanique nécessite aussi des données personnelles, et même des données sensibles (données sur la santé). L'expert devrait au minimum savoir que la personne souffre d'un traumatisme de ce genre. Le traitement de données personnelles nécessite un motif justificatif. Si tel n'est pas le cas, il y a atteinte illicite à la personnalité. On ne peut notamment pas traiter des données personnelles contre la volonté expresse de la personne concernée. Par ailleurs, les données sensibles ou les profils de la personnalité ne peuvent non plus être communiqués à des tiers sans motif justificatif.
Si par exemple une compagnie d'assurance-responsabilité civile traite des données personnelles contre la volonté expresse des personnes concernées, il y a violation de la protection des données. En effet, dans la plupart des cas, il n'y a probablement pas de motif justificatif. Par ailleurs, si les données transmises sans motif justificatif sont sensibles, il y a aussi atteinte à la personnalité.
Enfin, aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des individus concernés devait s'en trouver gravement menacée, notamment du fait de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse. Il convient dans chaque cas d'étudier si la protection des données dans l'Etat en question est équivalente à celle pratiquée en Suisse. Néanmoins même dans un Etat disposant de règles de protection des données d'égale valeur ou même de valeur supérieure, il est difficile pour la personne concernée de faire valoir ses droits à l'étranger (système juridique différent, autre culture, langue, risques au niveau des coûts, etc.). A notre avis, il ne faut communiquer des données personnelles à l'étranger que s'il est effectivement impossible de procéder en Suisse à un traitement poursuivant le même but. Plus les données sont sensibles, plus il convient d'y veiller.

7.10. Clauses de consentement

La transparence du traitement des données dans le domaine des assurances privées demeure insuffisante. Nous soutenons donc les efforts qui tendent à répondre aux souhaits des consommateurs.

Les «procurations générales» sont encore d'un usage courant dans le domaine des assurances privées. Les assureurs s'appuient sur ce genre de clause pour traiter les données personnelles des assurés. Mais en général, l'assuré ne sait pas qui traite quelles données et dans quel but. Ces procurations sont donc nulles du point de vue de la protection des données. La portée de clauses de consentement révocables en tout temps doit être claire pour les personnes concernées. Si les

clauses de consentement sont prérédigées, le consentement court le risque de devenir une simple formalité.
Nous soutenons donc en matière d'assurance les efforts qui vont dans le sens des droits de la personnalité des assurés et notamment de la transparence. Il convient de se référer à ce propos à nos précédents rapports d'activités (4e Rapport d'activités, p. 177, 5e Rapport d'activités p. 183). En utilisant la clause de consentement, les assurances entendent demander non seulement des données personnelles aux autorités et à d'autres tiers, mais aussi délier les médecins de leur secret médical.
A ce propos, les représentants des médecins et des organismes d'assurance sont en train d'élaborer un projet fondé sur le secret médical, projet qui abonde dans notre sens. Nous pouvons le résumer ainsi: il repose sur le secret médical et la violation de celui-ci est sanctionnée par le code pénal. Le secret médical est également applicable à l'égard d'autres médecins. Il peut être levé avec le consentement de la personne concernée. La personne concernée doit pouvoir reconnaître la portée du consentement, lequel doit être requis dans chaque cas. Les clauses de consentement forfaitaires remises à l'avance sont nulles.
Le PFPD salue ce genre d'initiative, tout particulièrement dans un domaine où l'on traite des données sensibles.

7.11. Questionnaires trop détaillés dans le domaine des assurances privées

Nous avons constaté que diverses compagnies d'assurances utilisaient des formulaires dont le contenu était pratiquement semblable. Ces formulaires ont une caractéristique: ils contiennent un très grand nombre de questions sur la santé.

Des personnes privées tout comme des médecins nous ont signalé que certaines compagnies d'assurance utilisent des questionnaires pratiquement identiques. Les secteurs de l'assurance-vie et de la prévoyance semblent particulièrement touchés par ce phénomène. Ces formulaires contiennent un très grand nombre de questions sur la santé.
Nous citerons à titre d'exemple le formulaire «rapport d'enquête médicale» des compagnies suisses d'assurance-vie. Ce formulaire est manifestement utilisé lorsque quelqu'un désire être admis dans une caisse de pension. Il contient quelque 80 questions. Une partie de ces questions doivent en outre être remplies par un médecin imposé. Si le candidat à l'admission désire éviter les problèmes tant avec l'organisme de prévoyance qu'avec l'employeur, il n'a en pratique pas d'autre choix que de se soumettre à cette procédure.
La controverse porte sur le fait de savoir si ces formulaires, qui ne peuvent porter que sur la partie dite «supraobligatoire», sont encore compatibles avec la

protection des données. Nul n'ignore que dans le domaine des assurances privées également, seules les questions appropriées et nécessaires pour atteindre le but poursuivi sont autorisées.
Nous sommes donc en train de procéder aux études requises à ce propos auprès de l'Association suisse d'Assurances ainsi que de l'Office fédéral des assurances privées. Nous voudrions déterminer notamment si d'autres assurances en Suisse utilisent ce genre de formulaires ou des formulaires similaires. Par ailleurs, nous aimerions savoir si toutes les données sur la santé que les différentes compagnies d'assurance demandent à ce propos sont dans tous les cas nécessaires.

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

Les assureurs ont l'intention de renforcer les mesures contre l'abus en matière d'assurance. Ils estiment nécessaire de prendre des mesures plus sévères dans l'intérêt même des assurés intègres. Du point de vue de la protection des données, il convient en particulier de respecter les principes posés par la loi fédérale sur la protection des données.

Selon les assurances, les demandes abusives de prestations d'assurances sont en nette augmentation. Ce phénomène serait dû entre autres aux difficultés économiques actuelles, à une mentalité de plus en plus revendicatrice et à une évolution du sens moral. L'Association suisse d'assurances (ASA) a donc mis sur pied un service chargé de lutter contre les abus en matière d'assurances.
Les données personnelles ne peuvent être traitées que s'il existe un motif justificatif. Il est légitime pour l'assureur de vouloir lutter contre les abus. Mais il est déterminant que cette démarche s'accompagne d'un respect des principes de protection des données. Ainsi, l'atteinte à la personnalité de la personne concernée pour atteindre le but en question doit demeurer proportionné (principe de la proportionnalité). Par ailleurs, les personnes concernées doivent recevoir le plus d'informations possible (principe de la transparence).
Le système central d'information (ZIS) par exemple a pour but de protéger les compagnies d'assurances des manœuvres frauduleuses. Il gère un fichier (enregistré chez nous) sur les procédures pénales et civiles pendantes et closes (cf. 4e Rapport d'activités, p. 181 ss). Le règlement du ZIS est en cours de remaniement auprès de l'ASA et sera ensuite soumis au PFPD qui examinera en premier lieu si les inscriptions prévues dans le ZIS sont effectivement appropriées et nécessaires. A nos yeux toutefois, il est déterminant que les personnes figurant dans le ZIS en soit informées. Elles peuvent d'une part faire effacer ainsi toutes les inscriptions erronées. D'autre part, le fait pour les personnes concernées de savoir qu'elles figurent dans ce fichier devrait avoir un effet préventif. Ce qui devrait être aussi dans l'intérêt des assureurs. Pour le reste, nous avons prié

l'ASA de nous informer de toute autre activité concernant l'abus dans le domaine des assurances.

7.13. Procédure d'admission auprès d'une assurance-perte de gain en cas de maladie et d'une caisse de pension

Au cours de la procédure d'admission auprès d'une assurance-perte de gain en cas de maladie et auprès d'une caisse de pension, les employeurs ont souvent la possibilité de consulter les données concernant la santé de leurs futurs employés. Ce procédé n'est pas compatible avec la protection des données.

Lorsqu'une personne commence à un nouvel emploi, elle doit en général faire une demande pour être admise auprès d'une assurance-perte de gain pour cause de maladie et d'une caisse de retraite. Il lui faut à cet effet remplir des formulaires standard comportant des questions sur son état de santé. En effet, les assurances-perte de gain peuvent en principe sélectionner les risques en procédure d'admission. Il en va de même de la prévoyance qui va au-delà de la prévoyance obligatoire.
Nous avons encore dû constater que plusieurs formulaires sont contraires aux principes généraux de la protection des données.
Les formulaires (comportant les questions relatives à la santé) doivent être remplis à la fois par l'employé (personne assurée) et par l'employeur (preneur d'assurance). L'employeur prend ainsi connaissance sans y être autorisé de données concernant la santé de l'employé (violation du principe de la proportionnalité).
Les formulaires de demande ne sont pas les seuls à contrevenir à la protection des données: dans un cas porté à notre connaissance, une caisse-maladie a informé l'employeur que son nouvel employé était séropositif et ne pouvait de ce fait être admis dans l'assurance-perte de gain pour cause de maladie qu'avec une réserve. Il est inutile d'expliquer que cela peut avoir – surtout actuellement – des conséquences très graves pour l'employé. Nous estimons que l'employeur ne doit être informé de l'existence d'une réserve de l'assurance que si – du fait de la réserve - il doit payer le salaire à la place de l'indemnité pour cause de maladie (cf. également le rapport du groupe de travail «Protection des données et liste d'analyses/assurance-maladie» (ADAK), Aspects de la Sécurité sociale no 2/96, disponible auprès de l'OFAS).
L'ensemble de la question assurance/employeur nécessite un examen plus approfondi en ce qui concerne la protection des données. L'employeur est certes soumis à une forte pression au niveau des coûts et a un intérêt légitime à n'employer que des collaborateurs «sains» du point de vue de ces mêmes coûts.

Cela ne change rien au fait qu'il ne doit en aucun cas pouvoir prendre connaissance du questionnaire concernant la santé de l'employé.

8. Santé

8.1. Flux de données illicites dans le cadre des soi-disant formes d'assurances spéciales?

Conformément à la loi sur la protection des données, tout traitement régulier de données médicales doit explicitement être prévu par une loi. La LAMal cependant ne règle d'aucune manière les flux de données dans le cadre des formes d'assurance spéciales. Le problème de fond est que l'attribution des tâches aux divers acteurs impliqués dans ces nouvelles structures d'assurance ne sont absolument pas claires.

Les organes de la Confédération agissent sur la base de mandats légaux et conformément à ces derniers. C'est là le principe de la légalité qui a été concrétisé dans la jurisprudence des plus hautes instances judiciaires ainsi que dans les articles 17 à 19 de la LPD. Ces éléments concrets peuvent être décrits par deux constatations. Premièrement, les exigences envers le niveau et la précision des bases légales sont devenues plus contraignantes lorsque les données traitées sont sensibles et que le nombre de personnes concernées est élevé. Deuxièmement, le consentement d'une personne concernée peut justifier la légalité d'un traitement de données par un organe fédéral seulement si ce traitement constitue une exception. Les traitements qui doivent avoir lieu régulièrement doivent cependant pouvoir s'appuyer sur une base légale. Conformément à la LPD, les traitements de données médicales *doivent explicitement être prévus dans une loi au sens formel*.
C'est pourquoi dans le domaine de l'assurance-maladie de hautes exigences doivent être formulées envers la précision des réglementations au niveau de la loi. En contraste avec ces exigences se trouve le fait que la loi sur l'assurance-maladie contient déjà pour l'assurance de base des éléments qui demandent à être expliqués plus en détail. Ce qui pourtant déçoit vraiment, c'est que les *flux de données* liés aux formes spéciales d'assurance ne sont *absolument pas réglementés* par la loi et qu'on se rend compte en étudiant cette dernière en détail qu'elle ne dit même absolument rien sur les tâches des divers acteurs impliqués dans de tels modèles.
Le PFPD n'est pas censé remplacer des bases légales qui font défaut par des autorisations de quel genre qu'elles soient, sans compter qu'il n'en a pas la compétence. Nous devons nous borner à attirer régulièrement l'attention de tous les acteurs avec lesquels nous entrons en contact dans le cadre de ces formes

spéciales d'assurance sur la nécessité d'une réglementation et sur les problèmes qui peuvent surgir au cas où le législateur resterait inactif.

8.2. Le modèle d'assurance Nova Light de la Swica

L'idée semble alléchante: un assuré limite son libre choix du médecin à ceux qui sont sélectionnés par l'assureur sur la base des tarifs avantageux de leurs prestations. Ceci permet à l'assureur de concéder à l'assuré un certain rabais sur les primes. Pourtant, le procédé de sélection ainsi que les bases des données soulèvent des questions d'un point de vue de la protection des données.

La presse, la publicité faite par la Swica ainsi que celle (opposée) en provenance du camp des médecins ont fait connaître la possibilité de contracter l'assurance-maladie obligatoire auprès de cet établissement à des primes réduites si l'on accepte en contrepartie de limiter le libre choix du médecin à ceux qui figurent dans la liste présentée par l'assureur. Cette démarche soulève non seulement des questions au niveau de la législation sur les cartels et de la politique de la santé publique, mais aussi du point de vue de la protection des données. Le PFPD a été consulté à ce sujet par un grand nombre de médecins. Nous avons étudié principalement deux questions, ayant dû laissé en suspens l'une d'entre elles.
La première question qui s'est posée était de savoir si la Swica est autorisée à consulter la statistique CAMS pour établir sa liste des médecins à tarifs modérés. Il faut préciser ici que le fichier appelé « Statistique CAMS » contient des données relatives à tous les assureurs faisant partie du Concordat des assureurs-maladie suisses. Ceci pourrait à première vue constituer une violation du secret professionnel par d'autres assureurs ou par le maître de fichier. Nous ne partageons cependant pas l'opinion de l'Office fédéral des assurances sociales selon laquelle un assureur est autorisé à accéder à l'intégralité des données contenues aujourd'hui dans ce fichier parce qu'il y a lieu de préciser que dans cette collection de données seuls les prestataires sont identifiés, mais pas les patients. Elle ne contient donc pas de données sensibles telles que des données médicales spécifiques à une personne, ce qui signifie que la base légale sous forme d'ordonnance suffit pour justifier le traitement. Celle-ci existe à l'article 76 de l'ordonnance sur l'assurance-maladie qui prévoit que les assureurs peuvent traiter *en commun* certaines données à des fins clairement et limitativement définies. Parmi ces buts, on trouve également l'«analyse des coûts et de leur évolution», ce qui devrait bien justifier le but du traitement poursuivi par la Swica.

La deuxième question, qui concerne *l'exactitude et l'aptitude* des données utilisées, est au moins aussi importante. En ce qui concerne l'exactitude des données de la liste, il faut préciser que celle-ci n'était pas assurée, au moins pas d'emblée. Ainsi, la liste contenait un médecin qui était décédé depuis une année et demi et qui – bien évidemment – n'avait pas engendré beaucoup de coûts pendant la période de référence. Selon ses propres dires, la Swica étudie la possibilité de mettre à jour ces listes de médecins plusieurs fois par année, ce qui devrait permettre d'améliorer l'actualité des données. Quant à la question concernant l'aptitude des données utilisées, il s'agit certainement d'une question fondamentale. Ce qui est également certain, c'est que ce n'est pas en premier lieu une question touchant au domaine de la protection des données. Il s'agit plutôt de vérifier si l'on peut dire que cette sélection a été réellement opérée dans le but d'assurer une «réduction des coûts des soins médicaux» ce qui signifierait qu'elle remplit les exigences de l'article 41, al. 4 de la LAMal. Contrairement à la question concernant les bases légales pour les accès effectués, nous avons dû laisser en suspens cette question concernant l'aptitude et l'adéquation de la procédure de sélection. La réponse à cette question devra être trouvée en fonction de critères d'économie de santé publique en général et du procédé «Physician Profiling» en particulier.

8.3. Les traitements de données effectués dans le domaine de la santé publique sont à peine réglementés – considérant leur fréquence

On peut constater récemment un énorme accroissement du nombre de traitements de données dans le domaine de la santé publique. Ceux-ci ne sont cependant pas une conséquence des changements intervenus dans la LAMal. Nous constatons plutôt que les organes qui traitent les données justifient leurs exigences envers la fourniture de données par des interprétations très libres des termes plutôt flous de la législation actuelle. Cette tendance semble très problématique du point de vue de la protection des données, sans compter qu'elle est en conflit avec la légalité.

La constatation suivante n'est pas nouvelle: partout où un grand nombre de problèmes liés à la protection des données surgissent, le problème de fond réside souvent dans des *manques de clarté*, en particulier dans les *buts imprécis* des traitements. Ces imprécisions sont très nombreuses dans le contexte de la loi sur l'assurance-maladie. Ceci ne signifie pas que la loi en soi n'est pas bonne. Permettez-nous simplement de remarquer qu'il est inévitable – au vu des imprécisions conséquentes et des intérêts divergents des différentes parties impliquées – que les divers acteurs se permettent d'interpréter la situation de droit de

manière différente concernant d'importantes questions. Des imprécisions existent notamment au niveau de la délimitation des compétences entre la Confédération (assurance-maladie) et les cantons (établissements hospitaliers), mais aussi dans les rapports entre la planification et le marché sans oublier les imprécisions résultant de formulation trop vagues dans le texte de la loi. Nous allons illustrer ceci à l'aide des deux exemples ci-dessous.

Une des notions fondamentales de la loi sur l'assurance-maladie est celle de la *rentabilité* des prestations, rentabilité que les assureurs doivent pouvoir vérifier conformément à la LAMal. Etant donné qu'une définition concrète de cette notion fait défaut, on comprend bien la tendance des assureurs de ne pas définir ce terme de manière précise, mais de l'interpréter de manière aussi large que possible. On essaie ainsi de justifier des besoins relativement extensifs pour des consultations de données régulières. Or, il se trouve que la LAMal s'oppose à de telles exigences puisqu'elle ne permet de telles consultations de données dans les proportions demandées par les assureurs que dans des cas isolés et sur demande expresse. Un exemple qui prouve qu'il existe d'autres solutions est la liste de 64 diagnostics d'ordre général qui a été élaborée dans le cadre d'un accord de «Managed Care» entre un hôpital universitaire, le médecin-conseil et le service juridique de deux des plus grands assureurs-maladie. Des tests ont démontré que ces diagnostics d'ordre général étaient suffisants pour un échange régulier de données et – ce qui joue un rôle important pour les frais administratifs – ils peuvent être automatiquement dérivés des codes CIM-10 qui sont saisis dans les établissements hospitaliers à des fins statistiques (cf. annexe p. 376).

Une autre notion également vague est celle de la *surveillance*. Dans ce contexte, l'Office fédéral des assurances sociales (OFAS) demande des données, les assureurs jouant le rôle de fournisseurs de données. C'est la raison pour laquelle ces derniers penchent bien sûr à définir leur obligation de fournir les données de manière plutôt restreinte. En fait, la LAMal offre des indices pour une telle position, pour le moins en ce qui concerne le volume des données devant être livrées de manière régulière. De manière analogue à l'exemple précédent du contrôle de la rentabilité par les assureurs, la LAMal prévoit pour la fonction de surveillance de l'OFAS des pouvoirs très étendus de collecte de données *dans des cas isolés*. Dans certains cas précis et concrets, il est absolument légitime de «passer au crible» un assureur. Le volume des données devant être fournies de manière régulière – dans un certain sens à titre préventif – pour des tâches de surveillance n'est cependant pas définie dans la LAMal. Aussi longtemps que les buts des traitements à des fins de surveillance ne seront pas concrétisés, nous considérons qu'il serait problématique d'utiliser les données collectées à des fins statistiques également pour les tâches – insuffisamment définies – de surveillance. Un cas qui illustre bien les questions en suspens en ce qui concerne les compétences de surveillance de l'OFAS est le fait que plusieurs établissements hospitaliers ont interdit à l'Office fédéral de la statistique de transmettre les données qu'ils lui fournissent à l'OFAS à des fins de surveillance.

8.4. La carte à puce dans la santé publique: panacée ou placebo?

Après examen plus poussé, on constate que l'idée consistant à mémoriser des informations médicales sur une carte à puces n'est pas une idée bien réfléchie. En fait, non seulement des raisons juridiques et techniques de la protection des données, mais même des raisons médicales s'opposent à un tel projet. Quant au prétendu effet positif sur le coût de la santé publique, il n'est absolument pas établi.

Nous constatons – surtout ces derniers temps avec une fréquence accrue – des initiatives venant de cercles divers qui visent toutes à introduire une «carte à puce pour la santé publique». C'est pourquoi il y lieu d'apporter ici quelques mises au point au sujet des projets qui ont pour objectif de mémoriser des informations médicales sur une carte à puce. Permettez nous d'abord d'attirer l'attention sur le fait qu'un tel projet, de par son impact sur les libertés individuelles, exigerait un degré très élevé de légitimation démocratique, ce qui signifie qu'une base légale sous la forme d'une loi au sens formel serait une condition essentielle.
Il faut relever ensuite du point de vue de la protection des données que des problèmes graves relatifs à la protection de la personnalité ne sont pas évidents à prime abord et ne peuvent pas être résolus par de simples mesures techniques et organisationnelles. Quelle serait par exemple la mesure technique adéquate permettant d'exclure qu'un chômeur soit forcé lors d'une entrevue d'engagement à divulguer ses données médicales à son employeur potentiel ou à défaut de mettre fin à la discussion avec une issue négative pour lui, bien évidemment? Mais même au niveau des mesures techniques et organisationnelles, un certain nombre de réflexions seraient à faire. Ne citons par exemple que la transparence pour les personnes concernées (entre autres en garantissant un droit d'accès simple et exempt de frais) ainsi que le fait que les personnes concernées doivent être en mesure d'attribuer les droits d'accès de manière sélective.
Même du point de vue médical, ce n'est pas une bonne idée de vouloir stocker des données médicales sur des cartes à puce. Car il s'avère après examen plus approfondi que l'utilisation souvent prônée de telles cartes à puces comme carte d'urgence est une illusion. La première raison est que les urgences se produisent typiquement dans des endroits où l'on ne dispose justement pas d'équipement de lecture (en bon état de fonctionnement) pour lire cette carte, tel que sur la plage d'une île déserte, dans un avion, lors d'une course en montagne, etc. Deuxièmement et surtout, aucun médecin ne décidera de procéder à une transfusion sanguine en se basant uniquement sur les indications figurant sur une carte (à puce ou autre). Quant à d'autres utilisations, les données mémorisées sur de telles cartes ne peuvent souvent pas être considérées comme étant à jour avec une sécurité absolue. Si l'on considère par exemple les résultats d'une examen de laboratoire, on constate que l'on ne dispose de ces résultats souvent que

plusieurs heures après que le patient ait quitté le laboratoire (dans lequel il n'a peut-être même jamais mis les pieds). Etant donné que le concept d'une telle carte de secours part du principe que le patient porte constamment cette carte sur soi, il n'existe donc aucune possibilité réaliste d'assurer l'actualité des données.

Quant à l'aspect de la sécurité, on entend très souvent des appréciations positives concernant la carte à puce. Nous prétendons pourtant que les cas où le problème a vraiment été étudié à fond ont fait apparaître de sérieux doutes sur la sécurité de cette technologie (cf. par ex. Ross Anderson et Markus Kuhn, Tamper Resistance - a Cautionary Note, dans *The Second USENIX Workshop on Electronic Commerce Proceedings*, Oakland, California, 18 – 21 novembre 1996, pages 1-11, ISBN 1-880446-83-9; B. Schneier, A. Shostack *Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards,* publication prévue dans *First USENIX Symposium on Smart Cards, USENIX PRESS*).

Finalement, en ce qui concerne l'espoir que la carte à puce permette de réduire les frais de santé pour l'ensemble des assurés/patients, il doit être considéré avec beaucoup de circonspection. Premièrement, il est vrai que la présence d'un historique permettrait d'éviter les examens diagnostiques à double, mais il faudrait garantir que ce soient justement les actes inutiles qui soient empêchés, sans quoi la carte à puce aurait une influence négative sur la santé publique. Deuxièmement, une mise en œuvre de cartes à puce à grande échelle demande d'énormes investissements dans la phase initiale, ne serait-ce déjà que pour les équipements de lecture qui seraient nécessaires (sans compter que ces investissements seraient à refaire à chaque changement de technologie que personne ne peut exclure). Dans ce contexte, il est déjà presque ironique de constater que ceux qui aujourd'hui prêchent l'atout de la réduction des coûts sont précisément ceux qui ont l'intention de faire une bonne affaire avec l'introduction des cartes à puce. Pour conclure, nous tenons donc à souligner le fait qu'il n'existe aujourd'hui pas de chiffres permettant de prouver l'effet positif tant promis sur le coût global de la santé publique.

9. Génétique

9.1. L'avant-projet de loi fédérale sur l'analyse génétique humaine

Elaboré par une commission d'experts désignée à cet effet, sous l'égide de l'Office fédéral de la justice, l'avant-projet de loi fédérale sur l'analyse génétique humaine a été mis en consultation auprès des milieux intéressés jusqu'au 31 mars 1999. Outre les questions fondamentales de protection de la personnalité qu'il soulève, il en est une d'importance encore ouverte: celle du statut des échantillons. La nécessité du débat public a quant à elle été soulignée par les résultats de la discussion organisée à Bâle par le comité «Dialogue sur le diagnostic génétique - des spécialistes et des profanes s'entretiennent».

L'avant-projet de loi fédérale sur l'analyse génétique humaine

Nous avons été associés dès le début à ce projet en déléguant un représentant au sein de la commission d'experts. L'avant-projet de loi fédérale sur l'analyse génétique humaine vise à régler les conditions d'exécution de l'analyse génétique humaine, le sort des échantillons, ainsi que le traitement des informations génétiques en découlant. La protection de la dignité humaine et de la personnalité doit ainsi être garantie dans des domaines aussi divers que le domaine médical, celui du travail, des assurances, de la responsabilité civile, ainsi que dans les cas requis par l'identification d'une personne ou d'un cadavre.
L'avant-projet de loi fédérale sur l'analyse génétique humaine est le fruit d'un compromis entre les représentants des intérêts en présence au sein de la commission. Nous ne nous rallions de ce fait pas pleinement à toutes les options retenues, en particulier pour ce qui est des sections relatives aux rapports de travail et aux assurances. Pour les premiers, on peut en effet se demander si les rares cas dans lesquels une analyse présymptomatique peut être demandée revêtent un caractère suffisamment général et abstrait pour figurer dans une loi. Quant au secteur des assurances, le principe de «l'égalité des armes» a prévalu. Au nom de ce principe, et à certaines conditions, il est prévu qu'un assureur actif dans une branche d'assurance non obligatoire aura le droit de demander au preneur d'assurance, et à certaines conditions, le résultat d'analyses présymptomatiques reconnues fiables. La personne concernée devra également répondre à des questions sur ses prédispositions génétiques.
Certes, le fait que le secteur de l'assurance obligatoire ne soit pas touché est à saluer. Cette distinction est cependant relative pour deux raisons au moins: il est tout d'abord des cas où une assurance dite facultative est vitale pour l'intéressé et revêt de ce fait un caractère obligatoire. C'est le cas par exemple d'une

assurance-vie pour un petit entrepreneur en manque de liquidités désireux d'obtenir un crédit auprès d'une banque afin de sauver son entreprise. En outre, dans certaines branches d'assurance, il existe une grande perméabilité entre les secteurs obligatoire et non obligatoire, les données étant souvent traitées dans le même dossier pour des raisons d'efficacité. Dès lors, une information génétique peut être utilisée indifféremment dans l'un ou l'autre secteur, et ce à l'insu de la personne concernée.
Pour le reste, la problématique de la protection de la personnalité et des données personnelles a été abondamment débattue au sein de la commission. Les membres de cette dernière étaient sensibilisés à la nécessité de réglementer cette problématique par des dispositions spécifiques. Ceci a débouché sur l'élaboration de normes de protection des données particulières à chaque domaine traité par l'avant-projet de loi fédérale sur l'analyse génétique humaine.

Des doutes ont été exprimés par des représentants de l'Office fédéral de la justice quant à notre compétence formelle et matérielle en matière d'échantillons et de données génétiques sur la base de l'article 24novies de la constitution fédérale. Ces mêmes personnes sont en outre parties du principe que la législation fédérale et cantonale sur la protection des données n'englobe pas la protection des échantillons, ces derniers n'étant jamais mentionnés expressément.
Or, vu la lettre et l'esprit de l'article 24 novies, qui contient des indications assez précises en matière de protection de la personnalité, nous avons indiqué ne pas partager les doutes de l'Office de la justice. Nous avons en outre souligné que le législateur fédéral peut se fonder sur cette disposition pour étendre notre compétence aux organes cantonaux qui utilisent des échantillons et traitent des données génétiques. Pour le reste, les cantons seraient soumis à la surveillance des instances cantonales de protection des données (sous réserve des communications de données dans le cadre de la recherche médicale au sens de l'article 321bis du code pénal).
Vu les risques inhérents aux abus en matière génétique, il serait non seulement opportun de prévoir une instance de contrôle unique, le PFPD, garant d'une unité de doctrine, mais également d'adopter en la matière des règles uniformes de protection des données couvrant l'ensemble du territoire suisse. Ceci n'est pas seulement dans l'intérêt des personnes concernées, mais également dans celui des responsables de l'utilisation des échantillons et du traitement des données génétiques. Ces personnes seraient au clair quant à leurs obligations et n'auraient pas à se poser la question de savoir si elles agissent en tant que personnes privées, organes cantonaux ou fédéraux.

Les échantillons ne sont quant à eux pas mentionnés expressément dans la LPD, ni dans le Message du Conseil fédéral ou le commentaire relatif à cette loi. Il en va de même d'autres supports d'informations (disquettes, disques durs, bandes magnétiques ou autres). Le législateur a renoncé à une telle énumération afin que la LPD ne soit pas trop vite dépassée et soit applicable indépendamment de l'évolution technique. Il n'en demeure pas moins que la LPD englobe aussi bien la protection des données que de leurs supports. Une interprétation contraire viderait cette loi de sa substance.
Vu que la LPD s'applique dans les cas où l'avant-projet de loi fédérale sur l'analyse génétique humaine ne contient pas de dispositions spécifiques de protection des données génétiques, il doit en aller de même pour les échantillons. Ces derniers constituent des supports de données contenant une infinité d'informations, dont le degré de lisibilité dépend des analyses effectuées au sein d'un laboratoire ou d'un cabinet médical.
Nous sommes dès lors parvenus à la conclusion que l'article 5 de l'avant-projet de loi fédérale sur l'analyse génétique humaine devait être formulé en ces termes:

«Les échantillons et les données génétiques sont protégés par le secret professionnel (articles 39 de l'avant-projet, 321 et 321bis CP) ainsi que par les dispositions fédérales sur la protection des données applicables au secteur public.»

Il faut finalement garder à l'esprit deux points: un échantillon n'est tout d'abord jamais anonyme; on peut tout au plus le séparer de ses éléments d'identification. Ensuite, une des particularités des échantillons et des données génétiques est de ne pas concerner une seule personne, mais toute sa lignée. Un dérapage dans ce domaine peut déboucher sur la discrimination de groupes entiers de la population. Dès qu'une information est disponible, il est en outre difficile de résister à la tentation de l'utiliser, même si cette utilisation n'est en soi pas autorisée.
Un cas porté récemment à notre connaissance permet d'illustrer cette allégation: une personne a participé à une consultation génétique prédictive à des fins de recherche. Son médecin traitant a annexé le rapport de conseil génétique effectué dans ce cadre à un rapport d'assurance, et ce à l'insu de la personne concernée. L'assurance privée cocontractante, après avoir pris connaissance des prédispositions génétiques de l'intéressé, l'a accepté comme assuré, mais en émettant une réserve quant aux conséquences éventuelles desdites prédispositions.
L'assuré est intervenu auprès de son médecin pour protester. Le praticien a entrepris des démarches auprès de l'assurance, qui a finalement annulé la réserve. Cette histoire a une issue heureuse, car la personne concernée était informée de ses droits. Pour le reste, nous ignorons si l'assureur a détruit les informations génétiques entrées illégalement en sa possession, et nous ne

savons pas s'il a été fait usage de ce type de données envers des candidats moins informés.

Le dialogue sur le diagnostic génétique

Le comité «Dialogue sur le diagnostic génétique - des spécialistes et des profanes s'entretiennent» composé de 17 organisations et entreprises concernées par la génétique, a financé et organisé cette discussion, afin de porter cette problématique sur la place publique et d'ouvrir le débat. Ce dernier s'est déroulé en septembre et octobre 1998. Nous avons participé à la partie de la discussion relative au destin des données et échantillons biologiques collectés, ainsi qu'à leurs conditions de stockage, les critères et la durée de leur conservation. Nos interlocuteurs étaient inquiets des développements techniques et législatifs à venir. Les questions de l'intelligibilité et de l'accessibilité de l'information, ainsi que de la responsabilité pour la qualité de cette dernière, préoccupaient également les personnes présentes.
Outre le fait que nos interlocuteurs étaient comme nous d'avis que données et échantillons devaient être considérés comme un tout indissociable soumis aux mêmes critères de protection et sécurité des données, ce dialogue a prouvé le bien-fondé du principe du débat public ancré dans la Convention d'Oviedo que la Suisse devrait bientôt ratifier (Convention du Conseil de l'Europe sur les Droits de l'Homme et la biomédecine). Les participants nous ont en outre confortés dans nos convictions selon lesquelles les citoyens ont besoin d'être informés, et que cette information doit rester une de nos tâches prioritaires.

9.2. Commission d'experts pour la banque de données des profils d'ADN

Fin 1997, le Département fédéral de justice et police a instauré une commission d'experts pour la banque de données des profils d'ADN. La mission de cette commission d'experts était d'étudier s'il est indiqué de créer une banque de données de profils d'ADN pour l'ensemble de la Suisse.

Le 25 novembre 1997, le Département fédéral de justice et police a décidé l'instauration d'une commission d'experts pour la création d'une banque de données de profils d'ADN pour l'ensemble de la Suisse. Cette commission d'experts devait examiner s'il était nécessaire et adéquat de créer une banque de données contenant des profils d'ADN pour faciliter la poursuite pénale. La commission d'experts était composée de représentants des autorités cantonales pénales et de police, des universités, de l'Office fédéral de la police, de l'Office fédéral de la justice et du PFPD. La commission d'experts devait rédiger un rapport final à

l'intention du Conseil fédéral jusqu'à décembre 1998. Cela signifie qu'à compter de la séance constitutive à mi-janvier 1998, la commission d'experts disposait de 10 mois à peine pour se plonger dans cette matière difficile et complexe des profils d'ADN et pour la comprendre, pour apprécier tous les aspects importants liés à la création d'une banque de données suisse et finalement pour rédiger le rapport final. Dû à ce temps imparti très court, la commission d'experts n'a pas été en mesure de faire des déclarations sur le contenu des bases légales qui seraient nécessaires pour la création et l'exploitation de la banque de données des profils d'ADN.

Du point de vue de la protection des données, la problématique qui se pose est extrêmement délicate. Pour cerner les problèmes qui se posent, il est nécessaire de procéder à une analyse très différenciée et une appréciation des processus qui sont nécessaires jusqu'à ce qu'un profil d'ADN puisse être mémorisé dans une banque de données.

Prenons comme exemple la présence d'un homicide ou d'un abus sexuel. Sur le lieu du délit, les enquêteurs trouvent des traces de sang, de cheveux, de sperme, de salive, de peau. Sur un ou plusieurs des suspects on prélève un frottis de la muqueuse buccale. Cet échantillon biologique comme on l'appelle sera analysé dans un laboratoire pour établir un profil d'ADN. Un profil d'ADN se compose d'une combinaison alphanumérique comportant 2 lettres (XY pour masculin, XX pour féminin) et 26 chiffres. Cette combinaison alphanumérique est dérivée de la séquence non codante de l'ADN. Selon l'état actuel des connaissances scientifiques, cette séquence non codante de l'ADN ne fournit aucune information sur les particularités physiques, psychiques et intellectuelles ainsi que sur les prédispositions en matière de maladies de la personne concernée. La seule fonction possible aujourd'hui est qu'elle permet d'attribuer l'échantillon biologique à une personne précise. Après analyse de l'échantillon biologique, il est prévu de mémoriser ce profil d'ADN dans la banque de données des profils d'ADN. Aussi longtemps que le profil d'ADN n'est utilisé et stocké dans une banque de données que dans le but de pouvoir associer des traces prélevées sur le lieu du délit à une personne déterminée ou déterminable pour identifier un suspect comme étant l'auteur du délit ou au contraire pour le décharger de tous soupçons, le profil d'ADN peut – comme moyen d'identification – être comparé aux empreintes digitales. Ainsi, une banque de données contenant des profils d'ADN présente les mêmes risques et dangers que n'importe quelle autre banque de données contenant des données sensibles. Toute base de données dans laquelle des données sont introduites et traitées par des humains et qui est reliée à d'autres bases de données avec lesquelles des échanges ont lieu présente un danger d'abus. Il est par exemple concevable que des données mémorisées soient illicitement supprimées ou modifiées, que de nouvelles données soient introduites de manière infondée, qu'elles soient illégitimement communiquées à des tiers, que les transmissions de données par voie électronique soient surveillées ou interceptées.

Il ne faut cependant pas oublier que contrairement au prélèvement d'empreintes digitales, la création d'un profil d'ADN nécessite que l'échantillon biologique soit prélevé, analysé puis conservé. L'échantillon biologique recueilli par l'enquêteur ou prélevé sur des personnes suspectes permet cependant de récolter bien plus d'informations concernant la personne concernée que le profil d'ADN. Soumis à une analyse appropriée, l'échantillon biologique fournit notamment des informations sur les particularités physiques, psychiques et médicales de la personne concernée. Il en découle que le problème d'ordre éthique et juridique n'est en fait pas la banque des profils d'ADN elle-même. Les principaux problèmes se posent d'une part au niveau de la collecte (découverte sur le lieu du crime, frottis de muqueuse buccale prélevé sur un suspect) et du traitement (analyse, conservation). D'un autre côté, la possibilité de lier les données stockées dans une banque de profils d'ADN avec l'échantillon biologique dont le profil est issu ouvre la porte à des possibilités d'abus très étendues. On peut par exemple penser à la communication et la modification illicites des autres informations concernant la personne concernée qui peuvent être déduites de l'échantillon biologique et des données stockées dans la banque des profils d'ADN.

Ce n'est pas seulement au niveau des risques et dangers qu'il y a lieu de faire une distinction entre la collecte, l'analyse et la conservation de l'échantillon biologique d'un côté et le traitement du profil d'ADN dans une banque de profils d'ADN d'un autre côté. Cette même différenciation doit également être clairement faite en ce qui concerne les bases légales nécessaires. La collecte, l'analyse et la conservation de l'échantillon biologique relève de la compétence des cantons. Cela signifie qu'il faut se poser la question si les bases légales au niveau cantonal sont suffisantes pour permettre ces traitements d'échantillons biologiques ou si elles doivent éventuellement être d'abord créées. La question se pose en outre s'il n'est pas possible d'interpréter l'art. 24^{novies} de la constitution fédérale dans le sens que la Confédération a la compétence de fixer au niveau fédéral les conditions pour le prélèvement et la conservation d'échantillons biologiques par les cantons.

Si une banque de profils d'ADN doit être créée et exploitée au niveau fédéral, les considérations suivantes s'appliquent à la création des bases légales nécessaires:

la combinaison alphanumérique du profil d'ADN ne constitue pas, en tant que telle, une donnée personnelle au sens de la LPD aussi longtemps que la personne à laquelle appartient ledit profil n'est pas identifiée ou identifiable. Il suffit pourtant que l'échantillon biologique qui a servi à établir le profil d'ADN ait été trouvé en un endroit qui – avec une probabilité avoisinant la certitude – n'a pu être fréquenté que par une personne déterminée ou déterminable pour que ce profil d'ADN devienne une donnée personnelle. Si le profil d'ADN est enregistré dans une banque de données de pair avec un numéro d'identification PCN (**P**rocess **C**ontrol **N**umber, c.-à-d. numéro de contrôle de procédure), il

conviendra à plus forte raison de qualifier ledit profil de données personnelles. Si, au surplus une autre banque de données contient le même numéro PCN avec des informations personnelles telles que le nom, le nom d'emprunt (alias), le prénom, etc. on pourra en liant les deux enregistrements avec le même PCN des deux bases de données, immédiatement attribuer le profil d'ADN à une personne. Etant donné que la personne à laquelle le profil d'ADN appartient devient au moins identifiable, le profil d'ADN devient une donnée personnelle.

Si l'on stocke des profils d'ADN de personnes étant auteur ou victime potentiels d'un délit dans une banque de données de profils d'ADN, ces données personnelles stockées dans la banque de données doivent être qualifiées de données sensibles au sens de la LPD. Ceci peut également être le cas pour des profils d'ADN de personnes portées disparues aussi longtemps que la possibilité subsiste que la personne ait été l'auteur ou la victime d'un délit et que celui-ci fait l'objet d'une enquête de police. Il sera même nécessaire de considérer les profils d'ADN issus de traces prélevées sur le lieu d'un délit comme données sensibles au sens de la LPD puisque la possibilité existe qu'ils puissent un jour être attribués à une personne déterminée ou déterminable. Ce sont les raisons pour lesquelles la création et l'exploitation d'une éventuelle banque de données de profils d'ADN centralisée au niveau fédéral nécessite une base légale formelle. Si une réglementation par voie d'ordonnance basée sur l'art. 351^{septies} du Code pénal suisse devait être considérée comme suffisante au niveau politique pour une période de transition limitée jusqu'à la création des bases légales au sens formel, il y a lieu d'attirer l'attention sur le fait que le processus démocratique qui a lieu lors de l'élaboration d'une loi fédérale, est contourné. Selon la convention d'Oviedo (voir également 9.1. L'avant-projet de loi fédérale sur l'analyse génétique humaine), une discussion dans la population devrait au moins avoir lieu .
En ce qui concerne les conditions dans lesquelles des profils d'ADN peuvent être saisis et stockés dans une banque de profils d'ADN, les préposés cantonaux à la protection des données ainsi que le PFPD ont pris position à ce sujet dans une résolution(voir aussi page 348 Conférence suisse).

10. Crédits

10.1. Modification de la loi fédérale sur le crédit à la consommation

La création d'une banque centrale de données dans le domaine du crédit à la consommation entraînera fatalement le traitement d'un important volume de données. Le projet concernant une modification de la loi fédérale sur le crédit à la consommation prévoyait que le traitement des données personnelles serait soit régi par le biais de statuts, soit réglé par le Conseil fédéral. Pour des considérations relevant à la fois de la protection de la personnalité, de la transparence et de la sécurité du droit, nous estimons qu'il est impératif d'ancrer les dispositions relatives au traitement des données personnelles dans une loi au sens formel. A nos yeux, le traitement des données personnelles ne saurait être réglementé par de simples statuts. Une telle manière de faire équivaudrait pratiquement à signer un chèque en blanc. En notre qualité d'autorité de surveillance, nous ne pouvons pas défendre ce point de vue.

La création d'une banque de données unique dans le domaine des crédits à la consommation aura pour conséquence un traitement centralisé d'un volume considérable de données personnelles. Si cette innovation présente des avantages certains sur le plan de la rationalité et de la mise à jour des données, il n'en demeure pas moins que le maître de fichier sera investi d'un pouvoir considérable et assumera une responsabilité également importante en regard de la conformité des traitements aux dispositions de la protection des données. La centrale de renseignements sur le crédit à la consommation que le projet prévoit d'instituer, un service chargé de la mise en œuvre de tâches publiques au niveau de la Confédération, sera soumise à la surveillance du PFPD (art. 15a, 3e alinéa du projet de modification de la loi fédérale sur le crédit à la consommation). Lors de la procédure de consultation des offices, nous avons exposé les exigences en matière de protection des données mais celles-ci n'ont pas été portées à la connaissance du Conseil fédéral.
Ce qui nous préoccupait dans ce projet, c'était le fait que le traitement des données personnelles était réglementé par le biais de statuts (art. 15a et 15b de l'avant-projet de modification de la loi fédérale sur le crédit à la consommation). Notre expérience en matière de statuts appliqués au domaine privé permet de dire que les personnes concernées ne sont pas suffisamment informées. En outre, ces mêmes personnes sont souvent surprises, voire choquées, lorsqu'elles constatent que les données les concernant ne sont pas effacées bien des années plus tard. Les personnes concernées s'adressent régulièrement à nos services, surtout en rapport avec la collecte des données, la

communication des données à des tiers et l'annulation des données, et nous demandent parfois d'intervenir. L'élaboration de dispositions légales claires et précises, aisément accessibles pour l'ensemble de la population, permettrait de mettre un terme à bien des incertitudes. Conformément à l'article 15a, 2e alinéa de l'avant-projet de modification de la loi fédérale sur le crédit à la consommation, le Conseil fédéral arrête les prescriptions nécessaires en l'absence de statuts. Le projet de loi ne précise pas si, parallèlement aux données personnelles telles que le nom et l'adresse, des données sensibles, mesures de l'aide sociale entre autres, font également l'objet de traitements. Le traitement des données sensibles devrait être réglé dans le cadre d'une loi au sens formel et non par voie d'ordonnance (art. 17, 2e alinéa LPD). Notamment, il y aurait lieu de préciser dans la loi les données qui peuvent faire l'objet d'un traitement et à quelles fins, les tiers auxquels les données peuvent être communiquées, le maître de fichier responsable (dans le cas d'une société comptant de nombreux membres on peut aboutir à de très mauvaises solutions), la durée de conservation des données et les mesures techniques et organisationnelles destinées à assurer la protection des données (s'agissant des exigences d'une base légale, voir le 5ème rapport d'activités, p. 175-176, et le présent rapport p. 323).
Du point de vue du droit sur la protection des données, l'énoncé alternatif de statuts ou d'une ordonnance du Conseil fédéral ne constitue pas une solution satisfaisante. En effet, des statuts seraient uniquement approuvés par le Département fédéral de justice et police (art. 15a, 2e alinéa de l'avant-projet de modification de la loi sur le crédit à la consommation) et, partant, ne devraient pas satisfaire aux exigences d'une base légale. Par ailleurs, une autre question, celle de la communication des données de la centrale à la banque consentant une ouverture de crédit, resterait non réglée. En cas de procédure d'appel (en ligne), il faudrait au moins que celle-ci soit précisée dans le cadre d'une ordonnance. Enfin, pour le traitement de données sensibles par procédure d'appel, il y aurait lieu d'instituer une clause correspondante dans une loi au sens formel.
Forts de ces considérations, nous avons informé la Commission parlementaire de l'économie et des redevances des problèmes de protection des données qui se posent en relation avec la centrale de renseignements sur le crédit à la consommation.

10.2. Comparaison des données lors d'examens de crédit

Les entreprises actives dans le secteur de la vente par correspondance s'assurent en général de la solvabilité de leurs clients potentiels. Ce qui est déterminant en la matière, c'est la manière dont la situation financière des parties contractantes est examinée. Un examen de la solvabilité d'un client potentiel effectué dans l'optique de la conclusion

d'un contrat n'est licite que dans la mesure où les données personnelles sont interrogées ou comparées chez le maître de fichier, et cela de cas en cas. En l'absence de moyens techniques permettant une comparaison des données conforme à la protection des données, il n'est pas permis de communiquer globalement les adresses douteuses par supports de données.

Nous avons été informés que les traitements effectués par la société de renseignements économiques X ne répondent probablement pas aux principes de la protection des données. Il s'est avéré que des clients de la société d'encaissement Y se sont engagés à transmettre à cette dernière pour traitement tous les cas de recouvrements. Les données des débiteurs poursuivis par la société Y pour dettes et faillite ou au sujet desquels il existe des actes de défaut de biens sont ensuite communiquées à la société X. En contrepartie, afin de leur permettre de vérifier la solvabilité de leur clientèle, la société X livre régulièrement et globalement à certains de ses clients une liste actualisée des adresses à risques. Les données en question sont alors comparées par lots, avec les adresses figurant sur les commandes des nouveaux clients. La comparaison porte sur les nom, prénom, adresse, code postal et localité. Lorsque les données figurant sur les commandes et les critères bancaires coïncident rigoureusement, des listes négatives sont imprimées. Le client s'engage par contrat à n'utiliser les adresses à risque fournies par la société X que pour son propre usage interne et à ne pas transmettre ou vendre à un tiers ces informations. La société X a intégré dans ses données des «adresses de contrôle» dûment authentifiées par notaire pour prévenir un usage abusif des données. Si un abus devait tout de même être constaté, les adresses en question pourraient être produites comme moyen de preuve lors d'une éventuelle enquête.
Etant donné que la comparaison des données ne s'effectue pas auprès de la société X, maître de fichier, et qu'un certain nombre de données est communiqué aux clients, les méthodes de traitement utilisées sont susceptibles de porter atteinte à la personnalité d'un grand nombre de personnes. Le PFPD a exigé une modification du traitement et a émis une recommandation (texte intégral, voir p. 378) pour les raisons suivantes:
sur le plan économique, il est certes légitime de vouloir obtenir des informations sur la solvabilité d'un partenaire avec lequel on s'apprête à conclure un contrat. Le législateur a tenu compte de cet intérêt dans la LPD, à la condition toutefois qu'il n'en résulte pas d'atteinte illicite à la personnalité et que les principes généraux régissant la protection des données soient respectés. Le principe de la proportionnalité suppose en particulier que l'on traite autant de données que nécessaire, mais aussi peu que possible. La communication systématique, sans sécurité technique, de l'intégralité des données informatiques à des fins de comparaison des données est contraire au principe de la proportionnalité, à moins qu'il n'existe un motif justificatif.

Au nombre des motifs justificatifs énoncés à l'article 13, 2e alinéa, lettre c LPD, on trouve l'examen du crédit d'une autre personne. En vertu de cette disposition, il est interdit de traiter des données sensibles ou des profils de personnalité et seules peuvent être communiquées à des tiers les données dont ceux-ci ont besoin pour conclure ou exécuter un contrat avec la personne concernée. Toutefois, les adresses à risque ne sont pas directement vérifiées auprès de la société X; elles sont mises à la disposition du client globalement, contre paiement, sur supports informatiques, à des fins de comparaison des données. Cette manière de procéder permet non seulement de comparer les supports de données avec les noms de clients déterminés mais aussi d'utiliser n'importe quel autre nom. Ceci nous amène à dire qu'il s'agit là d'un élargissement du but du traitement, une question qui a déjà fait l'objet de controverses lors des travaux préliminaires de la LPD. Au terme de débats nourris, le Conseil des Etats et le Conseil national ont finalement refusé l'élargissement du but. A la lumière de ce qui précède, on peut donc dire que la communication sur supports informatiques de tout un segment de données en vue d'une comparaison constitue une communication de données qui dépasse largement le volume des données effectivement nécessaires à un traitement. Le législateur a expressément prévu à l'article 13, 2e alinéa, lettre c LPD qu'il est uniquement permis de communiquer à des tiers les données dont ceux-ci ont besoin pour conclure ou exécuter un contrat avec la personne concernée, à l'exclusion de toute autre donnée. Une comparaison des données ou un engagement, même pris par contrat, d'utiliser exclusivement des données pour son propre usage interne n'y change rien. Pour ces raisons, nous nous trouvons ici en présence d'une communication des données que ne légitime aucun motif justificatif.

Comme le PFPD a déjà eu l'occasion de le préciser dans une recommandation de 1994, il est interdit de communiquer systématiquement des listes globales d'adresses à risque ou de données négatives, avec mention du nom, de l'adresse et de renseignements quant à la situation financière (données concernant des poursuites pour dettes et faillite incluses) d'un client potentiel. (Voir 2ème rapport d'activité 1994/1995, p. 244 ss).

Les interrogations individuelles de données occasionnent fatalement un travail considérable pour les entreprises appelées à vérifier la solvabilité d'un très grand nombre de personnes. Pour cette raison, il y a lieu d'élaborer des solutions qui permettent de vérifier rapidement la solvabilité des clients tout en respectant les dispositions de la protection des données.

Le volume de travail supplémentaire incombant à la société X du fait de la comparaison des données doit être mis en relation avec la possibilité de contrôler d'éventuels traitements illicites ultérieurs de la part des clients de la société X. Vérifier les données de neuf clients au maximum par mois ne devrait pas occasionner un surcroît de travail considérable. L'inconvénient engendré n'est pas de taille face au risque que présente un éventuel traitement illicite ultérieur échappant à tout contrôle de la part des clients de la société X.

Les moyens techniques disponibles actuellement permettent en tout temps de comparer un support de données avec d'autres fichiers de données (p. ex: annuaire téléphonique électronique) et d'effectuer des copies de toutes les données pouvant être exploitées à des fins différentes de celles qui ont initialement été prévues. Rien, ni les engagements pris par contrat ni l'existence d'«adresses de contrôle» authentifiées par un notaire, ne peut efficacement empêcher cet état de fait. Par ailleurs, en l'absence de mesures de contrôle, un éventuel traitement abusif pourrait difficilement être constaté.
Pour que la communication de données en matière de crédits à la consommation soit conforme aux dispositions de l'article 13, 2e alinéa, lettre c LPD, il faut que les comparaisons de données se fassent chez le maître de fichier. Conditions préalables: la société X ne mémorise pas de nouvelles adresses et s'abstient d'utiliser les adresses à d'autres fins que celles prévues et le client se borne uniquement à vérifier la solvabilité des clients avec lesquels il entend conclure un contrat.

10.3. Cartes de crédit et clause de consentement

Depuis un certain temps déjà, nous demandons que les clauses de consentement soient présentées avec davantage de transparence. Nous estimons en effet que les personnes concernées doivent savoir à qui sont communiquées leurs données personnelles. Des représentants de la branche des cartes de crédit et les services du préposé fédéral à la protection des données se sont mis d'accord sur une formulation uniforme. Les formulaires de demande qui ne font pas état des conditions générales, c'est le cas notamment pour les formulaires proposés par voie de presse, ne sont pas conformes à la législation sur la protection des données. Lors de la signature d'un formulaire de ce type, le client n'est pas en mesure de prendre connaissance des conditions générales liées à l'utilisation de la carte. Au demeurant, la clause de consentement ne fournit pas suffisamment d'informations sur les traitements prévus.

Etant donné que les détenteurs de cartes de crédit ne savent généralement ni à quels traitements leurs données personnelles sont soumises ni à quelles communications ils s'exposent, nous demandons depuis longtemps déjà que les clauses de consentement en matière de cartes de crédit et les conditions générales (CG) y relatives fassent l'objet d'une transparence absolue.

Nous avons constaté que des journaux et autres périodiques publient régulièrement, par voie d'annonce, des formulaires de demande de carte de crédit. A chaque fois, la clause de consentement est extrêmement succincte et les CG passées sous silence. Nous avons remarqué également que les libellés se résument à quelques informations seulement et qu'ils sont formulés en termes très généraux. Ainsi, il arrive souvent que des demandeurs acceptent les CG et consentent à un traitement de leurs données sans avoir vu, au préalable, les CG. Pour cette raison, nous avons attiré à plusieurs reprises l'attention des organismes concernés sur le fait qu'un tel consentement est nul. Il se trouve que nous avons régulièrement affaire à des particuliers ayant appris fortuitement que leurs coordonnées figurent dans la banque de données du centre d'informations de crédits ZEK. Nous souhaitons donc que les détenteurs de cartes de crédit soient informés des traitements auxquels leurs données personnelles donnent lieu et à qui celles-ci sont communiquées. A cet égard, le centre d'informations de crédits ZEK, organisme auquel les banques communiquent entre autres des informations sur les refus de demandes de crédit ou de cartes de crédit, les blocages de cartes bancaires, les mesures d'encaissements en cours et les avis de pertes et qui conserve les données pendant des mois, voire des années, joue un rôle primordial. Le centre en question réunit une centaine de membres (entreprises) qui peuvent interroger les données disponibles en vue d'examiner la situation financière d'une personne qui dépose une demande de nouvelle carte de crédit.
Considérant que les organismes de cartes de crédit consacrent généralement une double page A4 à la publicité proprement dite, nous avons considéré comme non avenu l'argument selon lequel il n'y aurait pas suffisamment de place sur le formulaire de demande pour imprimer quatre à cinq lignes explicatives supplémentaires. Finalement, nous avons convenu, d'entente avec des représentants de la communauté d'intérêts des organismes de cartes de crédit, de la formulation suivante, qui doit figurer soit sur le formulaire de demande de carte de crédit, soit dans les CG:

«Je, soussigné, certifie que les informations ci-dessus sont exactes et autorise l'entreprise XYZ à demander aux services publics, à mon employeur, à ma banque et au Centre d'informations de crédits (ZEK) les renseignements nécessaires à l'examen de la présente demande. J'autorise également le centre à communiquer des informations en cas de carte bloquée, d'utilisation abusive de la carte ou d'arriéré de paiement qualifié.»

Nous avons par ailleurs suggéré de mettre en évidence, par des techniques spéciales, la clause de consentement et de la placer, par exemple, à la fin du formulaire de demande. Au demeurant, nous avons demandé que les CG fassent mention du traitement de données sur mandat et de la communication de données à l'étranger. En ce qui concerne le traitement de données sur mandat, nous

ne pouvons pas partager l'avis selon lequel le client n'a pas besoin d'informations supplémentaires dès lors que ce type de traitement est régi dans le cadre de la loi. La communauté d'intérêts des organismes de cartes de crédit étudie présentement la possibilité d'élaborer une solution unique. L'étude porte en particulier sur une présentation uniforme des formulaires de demande de carte, la mise en évidence par des techniques spéciales de la clause de consentement et la suppression de la pratique consistant à publier dans la presse des formulaires de demande, sans CG, par voie de petites annonces.

10.4. Droit d'accès «payant» dans le cadre de contrats d'ouverture de crédit

En règle générale, une demande de renseignement n'occasionne pas de frais pour le demandeur. Il peut y avoir des exceptions à cette règle lorsque les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande et que ce dernier ne peut justifier d'un intérêt légitime ou encore lorsque la communication des renseignements occasionne un volume de travail considérable. Les accords concernant les frais convenus par contrats sont nuls lorsqu'ils sont contraires à la législation sur la protection des données.

Une société de recouvrement s'est adressée à nos services pour savoir s'il est juste qu'une banque ne donne pas suite gratuitement à une demande d'information selon l'article 8 LPD. La banque concernée aurait affirmé que les extraits de comptes portant sur des conventions de prêt ou sur des contrats d'ouverture de crédit ne constituent pas des données personnelles au sens de la LPD. En outre, la banque aurait renvoyé la requérante à ses conditions générales, lesquelles stipulent expressément que les données sont fournies moyennant le versement de 15 francs par extrait.
La LPD énonce dans sa disposition régissant le droit d'accès que les renseignements sont, en règle générale, fournis gratuitement. Une participation équitable aux frais peut cependant être demandée exceptionnellement lorsque les renseignements désirés ont déjà été communiqués au requérant dans les douze mois précédant la demande et que ce dernier ne peut justifier d'un intérêt légitime ou encore lorsque la communication des renseignements demandés occasionne un volume de travail considérable. La banque défend le point de vue selon lequel les extraits de compte constituent des données comptables et que celles-ci, en vertu des dispositions contractuelles, sont exclusivement livrées moyennant le versement de 15 francs par extrait. Le fait que l'autorité cantonale chargée de la surveillance des crédits à la consommation ait approuvé la taxe de 15 francs

prévue pour les contrats d'ouverture de crédit ne modifie ni la validité de l'article 8 LPD ni le devoir de fournir gratuitement des informations. Si les renseignements désirés n'ont pas déjà été communiqués dans les douze mois qui précèdent la demande, la perception d'émoluments se justifie tout au plus en regard du volume de travail considérable occasionné, par exemple, dans le cadre des crédits remboursables en plusieurs versements.

10.5. Enregistrement d'entretiens téléphoniques par des banques

Depuis l'entrée en vigueur de la révision du code pénal, seuls peuvent être enregistrés sans consentement préalable des personnes concernées les appels d'urgence adressés à des services d'aide, de sauvetage et de sécurité. Dans le domaine privé, l'enregistrement de conversations téléphoniques est autorisé pour autant que tous les participants aient été dûment informés de la procédure et qu'ils aient donné leur accord. Les grandes entreprises, en particulier, demandent généralement cette autorisation par voie de circulaires. Les enregistrements servent à la constitution de preuves et s'effectuent également dans l'intérêt du client.

Plusieurs personnes nous ont demandé si l'enregistrement d'entretiens téléphoniques tel qu'il est pratiqué par les banques depuis le 1.1.1998 est légal. La révision de l'article 179^{quinquies} du code pénal rend punissable tout participant à une discussion qui enregistre sur quelque porteur de son que ce soit un entretien non public sans en avoir au préalable informé les autres parties concernées. En vertu du nouveau droit, seul reste licite, sans consentement préalable, l'enregistrement d'appels d'urgence adressés à des services d'aide, de sauvetage et de sécurité. Ce cas de figure excepté, les personnes qui envisagent d'enregistrer leurs conversations ont l'obligation d'en informer au préalable leurs interlocuteurs. Précédemment déjà, les répondeurs téléphoniques le faisaient automatiquement (FF 1996 III 1411).
Les investigations que nous avons menées permettent de dire que plusieurs banques enregistrent exclusivement les entretiens téléphoniques ayant trait à des transactions spécifiques, notamment le commerce de titres, de devises, de billets, de métaux précieux, de matières premières, de produits «OTC», etc. Les enregistrements s'effectuent uniquement à des fins de conservation de preuve et les clients sont informés par circulaire de ce traitement des données. L'information des nouveaux clients s'effectue lorsque ceux-ci entrent pour la première fois en relation avec les secteurs d'activité correspondants. Par ailleurs, les projets d'émissions et descriptifs de produits avec numéro d'appel mentionnent un éventuel enregistrement des appels. Pour ce qui précède,

l’enregistrement d’entretiens téléphoniques par des banques est conforme aux prescriptions de la LPD.

10.6. Publication et affichage de «listes noires» sur Internet et en vitrine

On observe que les créanciers sont toujours plus nombreux à vouloir clouer leurs débiteurs au pilori, comme au Moyen Age. La différence entre ces deux époques: le pilori a été remplacé par une diffusion des données via Internet ou un affichage en vitrine. La législation sur la protection des données prévoit dans ce domaine que la publication des noms de débiteurs est subordonnée à l’existence d’un motif justificatif. En l’occurrence, ce motif fait généralement défaut. Les personnes concernées peuvent demander au maître de fichier d’annuler sans délai les données ainsi publiées ou s’adresser au juge.

Pour la contraindre de rembourser une dette, une personne s’est vue menacée de poursuites judiciaires. Il lui a également été dit que son nom apparaîtrait sur la homepage Internet de son créancier. Le débiteur s’est adressé à nos services pour savoir si cette pratique est légale. Nous avons attiré l’attention du créancier sur le fait que la diffusion de données personnelles via Internet constitue une violation de la LPD, étant donné que ce traitement ne repose sur aucun motif justificatif. Nous lui avons par ailleurs demandé de mettre un terme à ses menaces et de suspendre la publication des données. Finalement, nous lui avons signalé que la personne concernée pouvait intenter une action en justice conformément à l’article 28 CC et que le PFPD était habilité à formuler une recommandation à son encontre. Les menaces ont cessé et aucun nom n’a plus été publié sur Internet.

Nous avons encore appris, cette fois par voie de presse, qu’un propriétaire de magasin affichait en vitrine le nom de ses débiteurs. En agissant de la sorte, il espérait certainement récupérer plus rapidement ce qui lui était dû. Presque à la même époque, une personne concernée s’est adressée à nos services pour dénoncer cette pratique. Nous sommes intervenus auprès du propriétaire du magasin pour lui signaler qu’aucun motif justificatif ne légitimait ce type de traitement. Depuis, le propriétaire du magasin s’est abstenu de mettre en vitrine le nom de ses mauvais payeurs.

11. Marketing direct et publicité

11.1. Méthode de collecte de données personnelles – les consommateurs fournissent naïvement des informations sur leur sphère privée !

Bon nombre de personnes semblent ne pas attacher d'importance à ce que l'on sait sur elles. Par exemple, elles remplissent sans sourciller des questionnaires sur les ménages émanant d'entreprises privées. S'ils agissent ainsi, c'est parce que souvent les consommateurs ignorent la manière dont sont structurées les activités de marketing, et surtout leur ampleur.

Catalogues de vente par correspondance, prospectus de voyage, concours, tirages au sort, atterrissent quotidiennement dans la boîte aux lettres de la plupart des ménages, sans oublier un flot de lettres publicitaires. Parfois, ces envois publicitaires sont accompagnés d'une lettre ainsi libellée: «Madame, Monsieur, Nous aimerions vous inviter personnellement à participer à un sondage auprès des consommateurs. En guise de remerciement, vous participerez à notre tirage au sort qui vous permettra de gagner peut-être un voyage ou une chaîne stéréo». Au bas de ce genre de missive, on trouve la plupart du temps discrètement placée et imprimée en petits caractères la phrase suivante: «Nous vous garantissons que vos données seront uniquement utilisées à des fins de marketing». Ce genre de clause de consentement imprimée en petits caractères doit être lue avec attention. Lorsqu'un doute subsiste à propos du but du traitement des données ainsi récoltées ou lorsque le but du traitement n'est absolument pas mentionné, il faudrait tout d'abord s'informer sur le but exact du relevé de ces données. Ces questionnaires associés à un concours sont un moyen très prisé par les organismes ou personnes désirant constituer un fichier pour appâter le public. Le particulier qui ne lit pas cette mention en petits caractères ou ne se pose pas de questions sur la valeur de ces cadeaux «appâts» livrera son profil de consommation ou de la personnalité plus vite qu'il ne le croit.

Aujourd’hui, de nombreuses personnes remplissent ce genre de questionnaires sans vraiment réfléchir, avec une certaine naïveté même, et ne semblent pas se soucier de savoir ce qu'il adviendra de leurs données. Le doute ne s'installe que bien trop tard - si jamais il s'installe -, lorsque déferle la première vague de publicité adressée personnellement et non souhaitée. Si elles agissent ainsi, c'est parce que la plupart d'entre elles ne connaissent pas suffisamment bien le domaine de la collecte de données. En effet, on ignore souvent que les sondages privés sur les ménages ont lieu la plupart du temps au profit d'entreprises. En outre, les entreprises les plus diverses participent au commerce des données personnelles. Les listbrokers ou les sociétés de marketing direct fournissent

contre rémunération des listes d'adresses qui sont constituées à l'aide de données collectées. Ces listes d'adresses sont établies pour la vente de certains produits ou services. Les critères de sélection appropriés à cet égard sont par exemple l'âge, le sexe, la profession ou le pouvoir d'achat.

Les personnes qui achètent volontiers par correspondance et le font régulièrement livrent ce faisant de précieuses informations sur leur comportement en matière d'achat et de paiement. Par ailleurs, les entreprises peuvent recueillir d'autres informations à partir de diverses sources publiques comme les registres du commerce et les annuaires téléphoniques, mais aussi en consultant des publications officielles ou des annonces parues dans les journaux. Les concours pour leur part livrent encore des informations supplémentaires.
Si l'on ne veut pas communiquer ses données personnelles ou ne désire pas trouver dans sa boîte aux lettres de la publicité que l'on ne désire pas, il faut se demander face à ce genre de sondage auprès des ménages s'il vaut vraiment la peine de participer à un concours couplé à un sondage. Nous recommandons en outre de joindre aux commandes par correspondance une lettre comportant la phrase suivante: «Je désire que mes données personnelles ne soient pas utilisées à des fins publicitaires ou pour des études de marché ou sondages d'opinion, et ne soient pas transmises à des tiers».

L'utilisateur doit se poser lui-même la question de la nécessité de participer à un concours s'il doit pour ce faire révéler le profil détaillé de sa personnalité ou son profil de consommation.

A propos des études de marché et sondages d'opinion émanant d'entreprises privées, voir en annexe la feuille d'information du PFPD, p. 368.

11.2. Envoi de publicité non souhaitée par courrier électronique

Cette forme de publicité nécessite l'adresse électronique (e-mail) du destinataire. La manière la plus courante de trouver ces adresses électroniques est de consulter les listes de destinataires, la composition des groupes de discussion ou les programmes spéciaux de navigation; on peut aussi se les procurer par le biais des réponses aux courriers reçus, sans oublier bien sûr la vente de ces adresses.

Il est facile d'identifier et d'enregistrer une personne dans Internet par le biais de son adresse électronique. Mais une adresse électronique peut aussi comporter d'autres informations sur le destinataire comme son nom, son prénom, son lieu de travail et son adresse personnelle. Grâce à ces renseignements sur la

personne, et le cas échéant grâce aussi à la participation des personnes concernées à des listes de destinataires ou à divers groupes de discussion, il est possible de cerner ses intérêts et d'établir ainsi un profil de sa personnalité. Ces données peuvent être exploitées par des tiers et utilisées à d'autres fins, par exemple pour l'envoi de publicité.
Lorsqu'il s'agit d'un envoi conventionnel de publicité par poste, on peut bloquer son adresse qui ne sera plus utilisée à des fins publicitaires (liste Robinson ou étoile dans l'annuaire téléphonique). Les expéditeurs d'envois publicitaires sont tenus dans ce cas de respecter le souhait d'une personne qui ne désire pas recevoir de publicité. La situation est tout autre dans le cas du courrier électronique. Bien que l'adresse soit valable dans le monde entier, il n'existe pas de liste centrale d'adresses où l'on pourrait, si nécessaire, la faire bloquer. Il est donc difficile de se protéger du courrier électronique non désiré. Aux désagréments crées par la publicité, s'ajoutent encore les taxes téléphoniques qui sont à la charge de la personne concernée.

Il convient donc de mettre en œuvre les moyens techniques adéquats pour protéger l'utilisateur du courrier électronique qu'il ne désire pas et qui, en outre, implique pour lui des coûts. Certains serveurs mettent à la disposition des utilisateurs des programmes contenant des filtres qui trient les messages électroniques entrants. On peut ainsi fixer les conditions dans lesquelles le courrier publicitaire est automatiquement effacé. Les filtres puissants dirigent eux-mêmes les envois publicitaires dans la corbeille à papier. Là aussi, un inconvénient n'en demeure pas moins: la publicité non désirée n'est reconnue qu'après avoir été chargée. Donc les frais de téléphone demeurent. Il est possible de remédier à cet inconvénient lorsque le tri se fait déjà au niveau du serveur.
La messagerie électronique a donc «son prix». Il est en effet long et fastidieux de se protéger des envois non souhaités.

Mais, indépendamment des envois publicitaires non souhaités, il n'est pas sans danger d'envoyer soi-même des données par courrier électronique. La plupart du temps, ces envois ne sont pas codés et peuvent être aisément lus, copiés ou modifiés par des tiers. Nous aimerions à cet endroit rappeler avec insistance que l'envoi de données non codées par l'intermédiaire d'Internet est tout aussi sûr et confidentiel que l'envoi d'une carte postale !

11.3. Associations: communication de listes de membres à des tiers

Les entreprises commerciales, les prestataires de services, les partis politiques ou les institutions à but non lucratif ont un intérêt certain à obtenir des adresses déjà sélectionnées selon des critères spécifiques. En effet, celui qui possède la bonne adresse est à même de proposer de manière ciblée son produit ou ses idées.

Il y a en Suisse autant d'associations à vocations diverses que de listes de membres ou de fichiers d'adresses. Celui qui souhaite vendre de la nourriture pour chiens, par exemple, peut s'adresser à toutes les associations d'élevage de chiens ou sociétés cynophiles de Suisse en vue d'obtenir des listes de membres, qui serviront notamment à l'envoi de matériel publicitaire. Ces listes d'adresses s'obtiennent généralement sans problème, qui plus est gratuitement. Par recoupement des données, les entreprises intéressées peuvent donc faire de substantielles économies.
Les innombrables questions qui nous ont été posées à ce propos révèlent que la facilité avec laquelle les données personnelles sont transmises irrite considérablement, et à juste titre, un grand nombre de membres d'associations. En effet, si les statuts d'une association ne le prévoient pas expressément, les organes compétents ne sont pas habilités à communiquer des listes de membres ou autres données personnelles à des tiers, à moins qu'ils n'y soient contraints par la loi ou qu'ils aient obtenu au préalable le consentement de leurs membres. Toute autre pratique constitue une violation de l'un des principes généraux de la LPD, à savoir celui de la finalité. Conformément à ce principe, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. Précisons également à cet endroit que la communication de listes de membres au sein d'une association est également subordonnée au consentement préalable des membres lorsqu'elle ne sert pas exclusivement à l'exercice des droits attachés à la qualité de membre (voir 5^{e} rapport d'activités, p. 203 ss, Communication de listes de membres).

11.4. Communication de données personnelles par des autorités communales à des fins commerciales

Un groupe de travail des préposés cantonaux à la protection des données, auquel participait également le Préposé fédéral à la protection des données, s'est penché sur le problème que pose la communication de listes d'adresses par les communes. Il s'agissait en particulier d'examiner dans quelle mesure et sous quelles conditions les autorités

communales peuvent communiquer des données personnelles à des fins commerciales et de dire si cette pratique se fonde sur une base légale suffisante.

Dans le cadre de nos activités sur le commerce d'adresses et le marketing direct, une même question revenait systématiquement, à savoir: l'origine des données traitées. Les entreprises et institutions auxquelles nous nous sommes adressés pour obtenir des précisions ont souvent mentionné, parallèlement aux fournisseurs privés d'adresses, les services du contrôle de l'habitant. Le traitement des données par des autorités communales relève de la compétence des cantons. Pour cette raison, nous dirigeons régulièrement vers les services cantonaux compétents les particuliers qui dénoncent auprès de nos services le fait que le contrôle de l'habitant de leur commune de domicile communique leurs données à des tiers, entre autres à des fins commerciales (sociétés commerciales, banques) ou philanthropiques (organisations chargées de récolter des dons).
Notre participation au groupe de travail des préposés cantonaux à la protection des données nous a donné la possibilité d'en savoir davantage sur la pratique cantonale en matière de communication de données à des fins commerciales. Par la même occasion, nous avons pu échanger des informations en matière de commerce d'adresses et de marketing direct.
Afin d'obtenir une vue d'ensemble des traitements effectués, le groupe de travail a élaboré un questionnaire à l'attention de toutes les autorités cantonales de protection des données. Les principales questions qui leur ont été posées sont les suivantes:

- une communication systématique des données personnelles à des fins commerciales ou philanthropiques est-elle envisageable? Dans l'affirmative, quels types de données font l'objet d'une communication et dans quel but?
- Ces traitements reposent-ils sur des bases légales?
- Les personnes concernées ont-elles la possibilité de s'opposer à ces traitements?
- Le droit d'accès et le droit d'obtenir rectification sont-ils garantis?

Etant donné que les cantons n'ont pas tous répondu à cette enquête, il n'a pas été possible de brosser un tableau exhaustif de la pratique dans ce domaine. Cela est dû au fait que, d'une part, il n'existe pas encore partout d'autorité centrale chargée de la protection des données au niveau des communes et, d'autre part, qu'une réglementation uniforme destinée aux autorités communales fait encore défaut. L'idée de départ, à savoir l'élaboration d'une réglementation uniforme minimale applicable à la communication, par les communes, de données à des fins commerciales ou autres, a donc dû être abandonnée.

Même si cette question relève de la compétence des cantons, nous souhaitons toutefois préciser ici qu'une meilleure information de la population en matière de traitements effectués par les cantons et les communes contribue à renforcer la sécurité du droit et la transparence. Cette observation prend toute son importance lorsque les données ne servent pas exclusivement à l'exécution des tâches prévues par la loi.

12. Statistique

12.1. Recensement 2000

Les Chambres fédérales ont approuvé le projet de révision de la loi fédérale sur le recensement. Parmi bien d'autres, deux nouveautés majeures se dégagent: la rationalisation de la méthode de relevé et la limitation du nombre des données utilisées pour la mise à jour des registres cantonaux et communaux.

Le prochain recensement aura lieu l'an prochain, en décembre 2000. Il s'agira d'un recensement transitoire qui ouvrira la voie au relevé de données à partir des registres. (cf. Rapport d'activités 1997/98, p. 206). L'an passé, l'Office fédéral de la statistique (OFS) a élaboré l'ordonnance sur le recensement fédéral de la population. Les nouveaux aspects liés au recensement fondé sur les registres y figurent déjà. Cette ordonnance reprend les principes mis au point lors du dernier recensement de la population de 1990, par exemple la définition des caractères d'enquête et auxiliaires ou la répartition des tâches entre Confédération et cantons. Parallèlement, elle renferme des nouvelles dispositions sur la préimpression de données sur les questionnaires et le recours à des centres privés de prestations de services auxquels une partie des tâches communales et fédérales seront déléguées. Les exigences de la protection des données que nous avions formulées dans l'optique de ce recensement dit de transition ont été incorporées à cette ordonnance. En particulier, les données nécessaires à l'harmonisation des registres des habitants y sont énumérées de façon exhaustive. Cette ordonnance prévoit par ailleurs la possibilité d'envoyer le questionnaire dûment rempli dans une enveloppe close séparée. Enfin, on y trouve des dispositions de protection des données à propos des tâches et devoirs des centres privés de prestations de services qui traitent des données personnelles dans le cadre du recensement de la population.

Des contrats-types pour la délégation de tâches aux centres de prestations de services seront élaborés durant l'année en cours. Ces contrats-types ont notamment pour but de garantir que les centres mandatés prennent les mesures nécessaires pour garantir la protection des données. Il est essentiel à cet égard que les données du recensement ne soient pas «enrichies» par des données personnelles extraites des fichiers auxiliaires du centre de prestations de services. En d'autres termes, le traitement des données par le centre mandaté ne doit pas se traduire par un reflux vers les cantons et les communes de plus d'informations que ces derniers n'en avaient reçu des agents recenseurs. Le reflux de données émanant des centres de prestations de services vers les registres doit donc strictement demeurer dans le cadre prévu par la loi. Par ailleurs, il convient d'exclure expressément de ces contrats – même si cela peut paraître évident – une actualisation des fichiers auxiliaires utilisés par les centres de prestations de services, à partir des données du recensement.

II. AUTRES THEMES

1. Datawarehousing, datamining

1.1. Datawarehousing, datamining et protection des données

Le datawarehousing et le datamining sont des procédés électroniques de traitement des données. Ainsi, une entreprise obtiendra, à partir d'ensembles de données apparemment sans rapport réciproque, des résultats intéressants. Ces procédés permettent d'étudier à quelles autres fins on peut utiliser les données personnelles disponibles. Les personnes concernées sont dans l'incapacité de reconnaître à quelles fins leurs données sont utilisées. Le principe de finalité n'est plus respecté.

Bon nombre d'entreprises souhaitent tirer davantage profit des données personnelles dont elles disposent sur leurs clients. Néanmoins, pour pouvoir fournir d'autres informations, ces données doivent être traitées et exploitées de manière appropriée, c'est-à-dire à l'aide de procédés permettant d'en extraire de nouvelles informations. Grâce aux découvertes les plus récentes de la technique, on peut utiliser les données personnelles nouvellement générées dans les buts les plus divers. Par exemple, elles peuvent contenir des messages cachés sur les expériences commerciales moyennes avec certains clients ainsi que des pronostics sur certaines personnes. Pour cette raison, ces technologies sont un

moyen prometteur permettant à l'entreprise d'utiliser ses données disponibles à d'autres fins potentielles.

La perte de transparence que cette évaluation permanente des individus implique pour la personne concernée pose un problème. L'individu n'est plus en mesure de juger quelles informations sont traitées dans quel but et par qui. La détermination des habitudes et des modes de comportement d'une personne grâce à la saisie, à la sauvegarde et à l'exploitation de données permet de constituer des profils de la personnalité riches en informations sans que la personne concernée en soit informée. On risque ce faisant d'enregistrer des données erronées. Or, puisque les personnes concernées n'ont en général pas connaissance de ce genre de traitement de données, elles n'ont guère la possibilité de contrôler l'exactitude de ces données ni d'exiger leur rectification.

Dans le cas des fichiers constitués sur la base de ce genre de procédés, il n'est guère possible de tenir compte de la nécessité de transparence. Les personnes concernées n'ont donc plus du tout leur mot à dire sur le sort réservé à leurs données. Le principe de la finalité lui non plus n'est pas respecté. En effet, lors du relevé des données, il est peu probable que le but du traitement soit visible pour la personne concernée ou qu'elle en ait été informée.

En vertu de l'art. 13 LPD, une atteinte à la personnalité n'est pas illicite si l'on peut faire valoir un motif justificatif. En général, pour pouvoir faire valoir un tel motif, il faut que les données soient nécessaires pour atteindre un but légitime précis. Dans le cas présent, il serait difficile de trouver un motif justificatif au sens défini par l'art. 13 LPD afin de légitimer une violation du principe de la finalité. Avec le datamining et le datawarehousing, ni les données, ni les résultats de l'exploitation à des fins économiques précises ne sont directement nécessaires. Pour cette raison, la compilation et l'analyse de données personnelles n'est pas sans poser un problème du point de vue juridique. La constitution de fichiers relatifs à des personnes dont les données ont été obtenues au moyen de datewarehousing ou de datamining n'est pas compatible avec les principes généraux figurant dans la LDP. Cela ne signifie pas que les entreprises doivent entièrement renoncer aux méthodes de marketing ou à la constitution de profils de marketing taillés sur mesure. Lorsqu'une entreprise exploite ainsi ses données, les personnes concernées doivent être informées avec exactitude et en priorité sur les méthodes de traitement et sur les buts de ce traitement. Elles peuvent ainsi si elles le désirent s'opposer au traitement.

2. Cartes-client

2.1. Carte-client M-Cumulus

Les habitudes d'achat des personnes qui utilisent une carte M-Cumulus sont exploitées, avec le consentement des intéressés, à des fins de statistiques et de marketing. Ces traitements ont pour objectif de cibler les clients et de leur adresser uniquement des informations publicitaires correspondant à leur profil. Le détail des informations n'est pas mémorisé dans les succursales. En cas de réclamation portant sur le nombre de points M-Cumulus crédité à un client, seul le Call Center est en mesure de dire si le calcul est exact.

On nous a souvent demandé si le traitement des données personnelles effectué dans le cadre de la carte M-Cumulus se déroulait correctement. Pour cette raison, le PFPD s'est rendu sur place et a assisté à une démonstration. Les traitements concernent uniquement les données personnelles fournies par les clients au moment de la demande d'une carte M-Cumulus. Il s'agit en l'occurrence du nom, du prénom, de l'adresse et de la langue de correspondance, d'autres informations, notamment la date de naissance et les personnes faisant ménage commun avec le demandeur, étant facultatives. Les produits achetés par le consommateur sont classés par groupes (d'habitudes / d'achat) à des fins de statistiques et de marketing. Objectif visé: adresser uniquement au client des publicités pour des produits qu'il est effectivement susceptible d'utiliser. Il est, par exemple, inutile d'envoyer à des retraités des offres pour une promotion de couches-culottes pour bébés. L'analyse du comportement d'achat permet de dire si une personne a des enfants, un jardin, des animaux domestiques, etc. De cette manière, une offre pour une tondeuse à gazon ne sera adressée qu'aux personnes possédant un jardin. Pour l'instant, il n'est pas prévu d'autres types de traitements. La personne qui refuse les informations de marketing et qui souhaite uniquement collectionner les points auxquels elle a droit ne reçoit pas de publicités. Néanmoins, les données en question sont aussi classées, mais de manière anonyme, dans des groupes de comportement bien précis. Les personnes qui s'opposent catégoriquement à tout traitement de leurs données n'ont pas la possibilité de collectionner des points (voir également 5ème rapport d'activités, p. 210-212).
Le maître de fichier nous a expliqué que seule l'adresse d'un client (sans son numéro de client) peut être utilisée par d'autres entreprises du groupe Migros, ceci exclusivement à des fins publicitaires. Par principe, aucune information n'est fournie à des tiers. Il est arrivé que des cambrioleurs aient oublié leur carte M-Cumulus dans un appartement 'visité'. Si, dans le cadre d'une instruction, un

juge s'adresse à la Migros pour obtenir le nom et l'adresse correspondant au numéro d'une carte M-Cumulus, celle-ci a l'obligation de lui communiquer les informations souhaitées.
Les succursales Migros ne mémorisent pas de données individuelles. Celles-ci sont stockées sous la forme de groupes de données (records) qui sont consultées en cas de réclamation portant sur le nombre de points crédités. Les réclamations peuvent être annoncées au Call-Center, qui en prend acte (texte libre). Pour des impératifs de protection de la personnalité, nous conseillons d'éviter autant que faire se peut les textes libres.

3. Protection des données et médias

3.1. Droit de requérir une rectification des données selon la loi sur la protection des données

On nous a souvent demandé si, dans le cas d'une diffusion de données inexactes par les médias, les personnes concernées pouvaient, parallèlement au droit de réponse prévu dans le cadre du droit civil, faire valoir un droit à une rectification selon la loi sur la protection des données.

La publication de données personnelles par la presse, la radio ou la télévision est assimilée à un traitement des données au sens de la LPD. Par conséquent, lorsqu'ils diffusent des données personnelles, les médias ont aussi l'obligation de respecter les principes applicables en matière de protection des données (licéité, principes de la bonne foi et de la proportionnalité, finalité et exactitude des données).
Un traitement de données est toujours considéré comme illicite lorsqu'un maître de fichier traite, en toute connaissance de cause, des données inexactes. Le droit de la personne concernée de demander une rectification des informations fournies n'est pas lié à une notion de faute. Comme nous avons déjà eu l'occasion de le préciser, un maître de fichier a le devoir de s'assurer de l'exactitude des données qu'il traite. Une personne peut donc demander à un maître de fichier de rectifier les données inexactes la concernant. Contrairement aux prétentions fondées sur l'article 15 LPD, le maître de fichier ne dispose pas de possibilité de justification au sens des articles 12 et 13 LPD. L'article 5, 2^{e} alinéa LPD doit être considéré comme une disposition qui légitime par elle-même une demande en rectification, dont l'application peut être prononcée par un juge en vertu de l'article 28a, 2^{e} alinéa CC.
Il existe différents types de données inexactes. Il y a des données totalement incorrectes (p. ex: nom mal orthographié, fausse date de naissance) et des don-

nées qui sont en soi exactes mais qui, réunies, donnent une vision partielle, voire fausse, de la réalité. La question de savoir dans quelle mesure l'exactitude relative de données personnelles doit, dans une situation précise, être assimilée à des données inexactes au sens de la LPD ne peut être tranchée qu'en considérant la finalité et la manière de traiter les données.
Le droit de réponse permet à la personne concernée d'exprimer son propre point de vue en rapport avec des faits la concernant (p. ex: publication d'un article dans un journal). Par contre, le droit de rectification se justifie et n'est seulement possible que pour une affirmation objectivement vérifiable.
Etant donné que les personnes non initiées ne sont souvent pas en mesure de dire si les éléments à rectifier constituent des données objectivement inexactes ou une présentation des faits perçue comme subjectivement inexacte, nous conseillons, par mesure de sécurité, d'agir sur les deux plans.

4. Domaine des douanes

4.1. Projet d'informatisation du transit commun douanier

La Direction générale des douanes nous a demandé de participer aux travaux engagés avec la Commission de l'Union européenne visant à une informatisation du transit commun douanier. Cette collaboration a permis d'introduire, dans le cadre du projet de révision des appendices de la Convention sur le transit commun, des normes de protection des données spécifiques pour le Nouveau Système de Transit Informatisé. En complément à cette législation internationale, nous avons rappelé à la Direction générale des douanes la nécessité d'entreprendre également les démarches visant à réglementer dans une ordonnance le traitement des données du transit au niveau national. La phase d'exploitation pilote du Nouveau Système de Transit Informatisé à laquelle la Suisse prendra part est planifiée pour l'automne 1999.

La Direction générale des douanes (DGD) nous a demandé, en collaboration avec le Bureau de l'intégration et l'Office fédéral de la justice, de participer aux travaux engagés avec la Commission de l'Union européenne (UE) visant à informatiser le transit commun douanier. Depuis l'entrée en vigueur du marché intérieur de l'UE en 1993, de nombreux problèmes sont en effet survenus dans le cadre du transit communautaire douanier. En février 1997, une commission d'enquête du Parlement européen a publié dans un rapport de nombreuses

recommandations préconisant principalement trois types de mesures: des mesures opérationnelles visant à une amélioration de la gestion de la procédure de transit; des mesures normatives ayant pour objectif une harmonisation des dispositions du transit communautaire; enfin une informatisation du transit commun ayant un effet de rationalisation du transit tant auprès des partenaires des douanes (ex: importateurs, transporteurs, ...) que des autorités douanières nationales.

Eu égard à sa position géographique, la Suisse a investi de nombreuses ressources dans l'élaboration du projet de Nouveau Système de Transit Informatisé (NSTI) appelé à devenir la pierre angulaire du système de l'échange européen de biens. Dans le cadre de ces travaux, de nombreuses discussions ont eu lieu avec la Commission de l'UE afin d'ancrer légalement ce nouveau mécanisme de transit. Il a ainsi été notamment décidé de procéder à une révision des appendices I à III de la Convention relative à un régime de transit commun passé en 1987 entre la Communauté économique européenne et les pays de l'AELE.

Participant au groupe de travail mis en place par la DGD, nous avons dans un premier temps examiné les implications juridiques au niveau national et international ainsi que les exigences de protection des données liées à ce projet, tant pour l'exploitation pilote que pour le système définitif. Les résultats de ces travaux ont démontré la nécessité d'ancrer ce projet d'informatisation dans des bases légales adéquates et d'intégrer les normes de protection des données nécessaires dans la révision en cours des appendices I à III de la Convention sur le régime de transit commun. Nous avons dans une seconde étape soutenu la DGD dans ses démarches auprès des différentes directions concernées de la Commission de l'UE.

Suite à ces différentes démarches et aux négociations qui ont suivi nous avons pu obtenir, en complément à la disposition sur la sécurité des données, qu'un article spécifique à la protection des données soit également intégré dans le cadre de la révision des appendices I à III de la Convention. Les points suivants ont ainsi été réglés: une définition des données personnelles englobant les personnes physiques et morales, une limitation de l'utilisation des données uniquement aux fins d'application de la Convention sur le transit, des exceptions à ce principe clairement définies, l'obligation pour les parties contractantes de mettre en place des mesures au moins équivalentes aux principes de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe ainsi que la mise en place de mesures de contrôle.

Le dénouement positif de ces démarches auprès de la Commission de l'UE a permis à la DGD de mettre en consultation en novembre 1998 une proposition à

l'attention du Conseil fédéral visant à accepter la révision des appendices I à III de la Convention relative à un régime de transit commun. L'objectif est en effet d'entamer la phase d'exploitation pilote du NSTI avec les bases légales nécessaires. Nous avons à cette occasion rappelé à la DGD qu'en complément à cette législation internationale, devraient encore être entreprises les démarches nécessaires visant à réglementer, au niveau d'une ordonnance, le traitement des données du transit sur le plan national.

La phase d'exploitation pilote du NSTI est planifiée pour l'automne 1999. Doivent y participer la Suisse et quatre pays membres de l'UE (Pays-Bas, Allemagne, Espagne et Italie). Après différentes étapes d'introduction du NSTI, l'application de la procédure de transit commun totalement informatisée est planifiée pour 2003.

5. Publication de données personnelles

5.1. Publication sur Internet de la liste des réfugiés accueillis en Suisse pendant la dernière guerre mondiale

En réponse à une interpellation Scheurer du 10 juin 1998, le Conseil fédéral prévoit de publier sur Internet la liste des milliers de réfugiés accueillis en Suisse pendant la dernière guerre mondiale. Appelé à se prononcer sur cette publication, le Préposé fédéral à la protection des données a mis sérieusement en doute la nécessité et l'opportunité d'une telle publication. Si celle-ci devait tout de même avoir lieu, le Préposé fédéral à la protection des données demande la création préalable d'une base légale et des mesures pour garantir les droits des personnes concernées. Plusieurs d'entre-elles ont d'ailleurs manifesté leur opposition à cette publication.

Le 10 juin 1998, le Conseiller national Scheurer a déposé une interpellation par laquelle il demande au Conseil fédéral s'il n'estime pas «qu'en réponse à des attaques violentes et pour mieux faire la lumière de manière objective sur notre passé récent, il conviendrait de publier la liste nominative exhaustive des réfugiés juifs et non juifs accueillis en Suisse alors qu'ils fuyaient la persécution nazie.»

Dans sa réponse, le Conseil fédéral estime «que la publication, sur Internet et en forme de livre, d'une liste des réfugiés admis en Suisse pendant la seconde guerre mondiale est utile pour enrichir la connaissance de l'histoire suisse de

cette époque. Compte tenu de la loi fédérale sur la protection des données, ce genre de publication nécessite une base légale expresse.» Celle-ci sera créée dans l'ordonnance d'application de la loi fédérale sur l'archivage adoptée le 26 juin 1998.

Appelé à prendre position sur le projet de réponse du Conseil fédéral, le PFPD a émis de sérieux doutes sur l'opportunité de publier une telle liste. Une telle publication est disproportionnée du point de vue de la protection des données. La publication sur Internet en particulier présente un risque plus élevé d'atteinte à la personnalité que la consultation auprès des Archives fédérales. Une publication non nominative est suffisante pour atteindre les buts visés par l'interpellation.

Si une publication sur Internet devait néanmoins être envisagée, elle nécessiterait au préalable la création d'une base légale explicite. En effet, une telle publication est une communication par procédure d'appel au sens de l'article 19, 3e alinéa de la LPD. Selon cette disposition, un organe fédéral n'est en droit de rendre des données personnelles accessibles au moyen d'une procédure d'appel que si cela est prévu expressément dans une base légale. Ni le règlement sur les archives fédérales, ni la future loi fédérale sur les archives ne prévoient expressément la publication de données personnelles par procédure d'appel. Préalablement à la publication, nous avons également exigé qu'un avis soit publié, notamment sur Internet, pour prévenir les personnes concernées ou leurs proches de la publication et de leur droit de s'y opposer. Enfin, à l'instar de notre recommandation relative à la publication des noms de personnes détentrices d'un compte en déshérence (voir 5ème Rapport d'activités 1997/98, p. 212), nous avons demandé à ce que la publication soit accompagnée de mesures de sécurité pour éviter des traitements abusifs. En particulier, la liste complète des 51'000 personnes concernées ne doit en aucun cas pouvoir être consultée en une seule interrogation ou télédéchargée. Cela implique que la consultation se fasse de cas en cas et selon des critères prédéterminés.

Dès la réponse du Conseil fédéral connue, plusieurs réfugiés de la dernière guerre ou leurs proches se sont plaints à nous et refusent de voir leur nom et celui de leurs proches publiés. Nous les avons informés de leurs droits et invité à faire connaître aux Archives fédérales leur opposition. Nous procéderons le moment venu à un contrôle pour vérifier que ce droit d'opposition est respecté.

5.2. Publication d'une liste de noms annexée à une ordonnance du Conseil fédéral

L'introduction dans le texte même d'une ordonnance ou en annexe d'une liste de noms de personnes contre lesquelles des mesures administratives sont prises doit respecter les principes généraux de protection des données, notamment le principe de proportionnalité, et doit être prévue par une loi au sens formel.

L'Office fédéral des affaires économiques extérieures (OFAEE) a soumis en consultation un projet d'ordonnance instituant des mesures à l'encontre de l'UNITA (mouvement d'opposition angolais). Le PFPD n'a pas été consulté directement. L'OFAEE, sur demande de la Chancellerie fédérale, nous a demandé dans un délai extrêmement court notre avis sur ce projet. Une liste de noms de dirigeants de l'UNITA ainsi que des membres de leurs familles était annexée à l'ordonnance. Ce projet posait des problèmes tant au niveau de la technique législative que de celui de la protection des données. Selon la doctrine, une ordonnance du Conseil fédéral comporte des règles générales et abstraites. Or, une ordonnance applicable uniquement à quelques dizaines de personnes ne remplit pas cette exigence. Pour cette raison, nous avons prié l'OFAEE de bien vouloir prendre contact avec l'Office fédéral de la justice afin de résoudre cette question de technique législative.
En ce qui concerne la protection des données, la publication des noms et prénoms de personnes contre lesquelles des mesures administratives sont prononcées (gel des avoirs et interdiction d'entrer ou de transiter) constitue un traitement de données sensibles. La LPD stipule que des données sensibles ne peuvent être traitées que si une loi au sens formel le prévoit expressément. Par loi au sens formel, on entend les lois fédérales, les arrêtés fédéraux de portée générale sujets au référendum ou les résolutions d'organisations internationales contraignantes pour la Suisse ainsi que les traités de droit international approuvés par l'Assemblée fédérale, comportant des règles de droit. A notre connaissance, une telle base juridique fait défaut. On peut également se poser la question de la nécessité d'une telle publication sous l'angle de la proportionnalité. Il faut procéder à une pondération des intérêts entre le but du traitement et l'atteinte nécessaire à la personnalité. Le traitement le plus «respectueux de la personnalité» doit être retenu. Dans le cas d'espèce, le but peut très bien être atteint par la seule communication de la liste des dirigeants de l'UNITA, des représentants de l'UNITA à l'étranger et des membres adultes de la famille des dirigeants de l'UNITA aux organes publics ainsi qu'aux personnes privées concernés. De plus, l'exactitude des données personnelles publiées n'est pas garantie.
En conclusion, nous avons recommandé à l'OFAEE de ne pas faire figurer cette liste nominative dans l'ordonnance instituant des mesures à l'encontre de

l'UNITA, ni dans le corps du texte, ni en annexe. Une telle liste doit faire l'objet d'une décision du Conseil fédéral, du Département fédéral des affaires étrangères, du Département fédéral de l'économie ou de l'OFAEE et être communiquée aux organes publics et personnes privées concernés. Nous avons également rappelé à l'OFAEE que le traitement de ces données sensibles doit être prévu expressément dans une loi au sens formel. L'OFAEE n'a pas tenu compte de nos observations et le Conseil fédéral a approuvé l'ordonnance en question.

5.3. Publication de données personnelles en relation avec des polices d'assurance en déshérence

Avant de publier quelque nom que ce soit en relation avec des polices d'assurance en déshérence, il convient d'épuiser au préalable toutes les voies susceptibles de permettre d'entrer directement en contact avec les personnes concernées. Le motif justificatif que constitue l'intérêt prépondérant privé ne peut être invoqué qu'en dernier recours pour légitimer la publication de données personnelles. En cas de publication des données sur Internet, il est conseillé de prévoir un accès par critères de recherche.

En relation avec la recherche de bénéficiaires de polices d'assurance en déshérence, on nous a demandé si les compagnies d'assurance étaient habilitées à publier une liste de polices d'assurance en déshérence, le cas échéant comment procéder pour ne pas violer les dispositions de la LPD.
La communication d'une liste de polices d'assurance en déshérence avec mention du nom du preneur d'assurance, de sa date et de son lieu de naissance, de la date et du lieu de la conclusion de la police, du nom de jeune fille pour les femmes mariées et du nom des bénéficiaires constitue un traitement des données au sens de la LPD. Par communication, on entend l'accès aux données, notamment le droit de consulter, de transmettre à des tiers et de publier des données. Le traitement de données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. On parle de traitement illicite lorsque des données personnelles sont traitées sans motif justificatif contrairement aux principes généraux régissant le traitement des données. Pour que les principes cités soient respectés, il y a lieu, d'abord, d'entreprendre tout ce qui est possible pour retrouver les bénéficiaires. Des informations concernant des bénéficiaires survivants ou leurs héritiers ne peuvent être publiées que si les personnes concernées ont, au préalable, manifesté leur accord quant à la publication prévue. Ce n'est qu'à partir du moment où les bénéficiaires n'ont pas tous pu être retrouvés que la publication des données pourrait se justifier en raison de l'existence d'un intérêt privé prépondérant.

Le mode de publication est toutefois fonction du nombre des bénéficiaires qu'il n'a pas été possible de retrouver. Si ce nombre est peu important, une publication dans les journaux uniquement constitue une mesure adéquate. En revanche, si le nombre des personnes restées inconnues est élevé, une publication des données sur Internet se justifie. Cela dit, un certain nombre de mesures de sécurité doivent être aménagées dans ce dernier cas afin de protéger les données contre un éventuel traitement non autorisé (mutation des données par exemple). En outre, les personnes concernées ne doivent pas avoir la possibilité d'interroger l'ensemble d'une liste. L'interrogation devrait être limitée à des cas précis, au moyen de critères de recherche définis, par exemple l'entrée du nom et de la date de naissance.

5.4. Mise à disposition sur Internet de données personnelles non sensibles par un organe fédéral

La mise à disposition sur Internet de données personnelles non sensibles par un organe fédéral doit être prévue par une ordonnance du Conseil fédéral. Une telle publication de données personnelles devrait être facultative et les personnes concernées informées des risques inhérents à la mise à disposition de données personnelles sur Internet avant de donner leur consentement.

La mise à disposition par un organe fédéral de données personnelles sur Internet constitue, d'une part, une communication par procédure d'appel nécessitant une base légale suffisante et d'autre part, une communication de données personnelles à l'étranger, y compris dans des Etats n'ayant pas de protection des données équivalente à celle qui est garantie en Suisse. La LPD exige que la communication de données personnelles non sensibles par procédure d'appel soit prévue expressément par la loi (au niveau d'une ordonnance du Conseil fédéral au minimum). Internet est un réseau ouvert sans instance centrale de contrôle qui veille au respect des dispositions de protection des données. A l'heure actuelle, aucune réglementation internationale ne peut garantir la protection des données et seul le droit du pays à partir duquel les données sont mises à disposition est applicable. La confidentialité n'est pas garantie. En effet, les données peuvent pratiquement de manière illimitée être copiées, modifiées, falsifiées ou bloquées. Comme l'utilisation d'Internet laisse des traces, il est aisé de constituer des profils de la personnalité à l'insu des utilisateurs. Par le biais d'Internet, il est également possible de pénétrer un ordinateur et de manipuler les données qui y sont contenues. Il faut dès lors informer les personnes concernées des risques inhérents à la mise à disposition de données personnelles sur Internet et donner à une telle publication un caractère facultatif. En plus de

l’exigence de la base légale suffisante, le PFPD est d’avis que la mise à disposition de données personnelles sur Internet doit être dans la mesure du possible facultative. Cela signifie qu’avant de donner leur consentement, les personnes concernées doivent être informées des risques inhérents à la mise à disposition de données personnelles sur Internet afin de se déterminer en toute connaissance de cause.

5.5. Danseuses de cabaret sur Internet

Les exploitants de cabarets ont récemment découvert l'Internet comme moyen de promotion pour leurs services. Si des images de danseuses permettant de les identifier sont montrées sur Internet, ceci présuppose un consentement préalable et explicite de la personne concernée.

Nous avons constaté que l'on trouvait sur l'Internet des photos avec nom (il s'agit partiellement de pseudonymes) de danseuses qui travaillent dans des cabarets suisses. Ces données accessibles par procédure d’appel (on line) permettent le plus souvent d'identifier les personnes concernées, il s'agit donc clairement de données personnelles.

La publication sur l'Internet a pour effet que ces données sont communiquées à l'ensemble de la planète. Il n'est pas autorisé de communiquer des données personnelles à l'étranger si ceci peut constituer une atteinte grave à la personnalité des personnes concernées, notamment parce qu'une protection des données équivalente à celle garantie en Suisse fait défaut dans les pays concernés. En outre, quiconque communique des fichiers à l'étranger est tenu d'annoncer ceci préalablement au PFPD s'il n'existe pas de base légale pour la communication et si les personnes concernées n'en sont pas informées.

Un exploitant de cabaret doit pouvoir invoquer un motif justificatif s'il veut traiter des données personnelles en infraction avec les principes de la protection des données. Dans le cas cité, le seul motif justificatif possible est le consentement explicite des personnes concernées. Ce consentement doit être accompagné d'une information claire et sans équivoque attirant l'attention sur le caractère global du réseau ainsi que sur les risques en matière de sécurité (en particulier la confidentialité, l'intégrité, la disponibilité et l'authenticité). Si une danseuse en qualité de personne concernée n'est pas d'accord que ses données soient publiées dans l'Internet, ceci doit dans tous les cas être respecté. Il ne doit pas en résulter de préjudices pour elle.

Nous avons invité les exploitants de cabarets à adapter, le cas échéant, leur pratiques aux dispositions légales.

6. Communication de données personnelles

6.1. Communication de données personnelles par un organe fédéral à une autorité cantonale

En dehors de toute procédure pendante (pénale, civile ou administrative) et en l'absence de toute base juridique, un organe fédéral n'est pas tenu de communiquer des données personnelles à un organe cantonal. Dans un tel cas, l'organe fédéral doit encore examiner si la communication est conforme aux principes généraux de protection des données.

Une jeune femme a eu un enfant d'un jeune homme dont elle connaît le prénom. Elle sait également que celui-ci est étudiant à l'Ecole polytechnique fédérale de Lausanne (EPFL). Le Code civil impose à l'autorité tutélaire (organe cantonal) de nommer un curateur chargé d'établir la filiation paternelle dès qu'une femme non mariée met au monde un bébé. C'est ainsi que l'autorité tutélaire a contacté l'EPFL (organe fédéral) afin d'examiner dans quelle mesure il était possible de déterminer l'identité du père éventuel. L'autorité tutélaire a demandé la liste des étudiants répondant au prénom recherché. L'EPFL a refusé, en dehors de toute procédure, de communiquer les renseignements demandés en invoquant la protection des données. L'autorité tutélaire et l'EPFL ont sollicité l'avis du PFPD. Nous avons ainsi proposé une solution tenant compte des différents intérêts en présence. Les photos numérotées des étudiants répondant au prénom recherché ont été présentées à la mère. Si une des photos avait été celle du père éventuel, seuls les nom, prénom et adresse de la personne correspondant à la photo auraient été communiqués.
Aucune procédure n'étant pendante, la LPD est applicable. Elle n'oblige pas l'EPFL à communiquer des données personnelles et même si les conditions requises sont entièrement remplies, l'organe fédéral doit encore examiner si la communication est conforme aux principes généraux de protection des données, notamment au principe de proportionnalité. Dans le cas d'espèce, la communication d'un nom, d'un prénom et d'une adresse respecte ce principe, ainsi que les dispositions régissant la communication. Il y est stipulé qu'un organe fédéral n'est en droit de communiquer des données personnelles que s'il existe une base juridique ou si le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale. La communication envisagée a donc été

considérée comme conforme aux dispositions de protection des données. Si une telle demande était intervenue dans le cadre d'une procédure pendante (pénale, civile ou administrative), elle n'aurait pas été régie par la LPD mais par les règles de procédure.

7. Protection des données et conditions légales cadres

7.1. Efficacité des modèles d'autorégulation sur la protection de la sphère privée

Pour la plupart, les lois européennes sur la protection des données permettent à toute personne de consulter les données enregistrées la concernant, de les faire rectifier et de décider de leur utilisation future. En cas d'usage abusif de ses données personnelles ou en cas de litige, elle peut se plaindre auprès d'une autorité indépendante ou faire valoir ses droits devant un tribunal. Aux Etats-Unis, si la protection des données n'est pas régie par le droit, il est par contre courant que des organismes économiques établissent des règles de comportement sectorielles pour le traitement de certaines données personnelles. Leurs membres ont toutefois la possibilité de suivre ces règles ou non (autorégulation).

Les modèles d'autorégulation visant la protection de la sphère privée sont certes une bonne chose; cela dit, pour garantir une protection effective, ils doivent remplir certains critères.
Grâce à ces modèles d'autorégulation, la personne concernée est informée des traitements envisagés concernant ses données personnelles ou peut donner son consentement au traitement de certaines données. A première vue, ce procédé pourrait constituer une solution optimale. Nul n'ignore cependant que dans la pratique, les personnes concernées sont en général assez rapidement prêtes à donner cet accord. Un refus leur fermerait souvent l'accès à certaines prestations (cartes de crédit, etc.). Dans un système dominé par l'autorégulation, les personnes concernées ne peuvent faire valoir leurs droits et leurs souhaits ne sont pas pris en considération. C'est surtout le cas lorsqu'il y a rapport de dépendance.

Certes la structure politico-économique du pays explique pourquoi les Etats-Unis n'ont pas de véritable loi sur la protection des données. Mais ce sont surtout les milieux économiques qui ont empêché une réglementation de la protection des données. A leurs yeux, les règles de comportement facultatives

sont suffisantes. Diverses études ont montré néanmoins qu'elles sont rarement respectées.

L'applicabilité est le principal critère permettant de juger de l'efficacité des règles de comportement sur la protection de la sphère privée. L'appréciation de cette applicabilité dépend essentiellement du pourcentage de membres de l'association en question qui respectent ces règles et de la possibilité d'imposer des sanctions à ceux qui ne les respectent pas. En outre, les règles de comportement doivent être transparentes, c'est-à-dire être rédigées dans une langue compréhensible par tous.

Toute personne désirant devenir membre d'un organisme économique devrait s'engager à respecter ses règles de comportement. Ce respect devrait être assorti de sanctions ou de contrôles externes contraignants. Enfin, il est extrêmement important que les personnes concernées ne soient pas laissées à elles-mêmes, mais bénéficient d'aide et de soutien. Par ailleurs, il faut intégrer aux règles de comportement un minimum de principes fondamentaux relevant de la protection des données, à savoir:

- information non équivoque des personnes concernées sur le genre de données relevées, le but dans lequel elles seront utilisées, leur destinataire et les possibilités de choix permettant de limiter leur utilisation et leur transmission.
- Octroi du droit de consultation et de rectification et mesures visant la sécurité du traitement des données.
- Possibilité de recourir auprès d’une instance indépendante.

7.2. Adaptation des bases légales aux exigences de la LPD

Aux termes de l’article 38, 3e alinéa de la LPD, les organes fédéraux étaient en droit de continuer à utiliser pendant cinq ans, à compter de l’entrée en vigueur de la LPD, les fichiers existants qui contiennent des données personnelles sensibles ou des profils de la personnalité, en l’absence d’une base légale au sens formel prévoyant expressément le traitement de ces données. Cinq ans après l’entrée en vigueur de la loi, plusieurs organes fédéraux n’avaient pas encore procédé aux adaptations légales nécessaires et le Parlement a été contraint de prolonger ce délai jusqu’au 31 décembre 2000. Deux messages seront présentés au Parlement cette année encore.

La LPD prévoit que des données sensibles ou des profils de la personnalité ne peuvent en principe être traités par des organes fédéraux que si une loi au sens formel le prévoit expressément. Cela vaut également pour les communications

régulières de telles données et en particulier lorsque des données sensibles ou des profils de la personnalité sont rendus accessibles par procédure d'appel. La base légale doit en règle générale définir les catégories de données sensibles qui sont traitées ou communiquées, les finalités du traitement, l'organe responsable du traitement et les organes qui participent, les organes ou personnes auxquels des données sont communiquées régulièrement, notamment par procédure d'appel, en précisant le but de la communication et son étendue. Dans une norme de délégation, le Conseil fédéral sera invité à fixer les modalités du traitement et notamment la responsabilité du traitement des données, l'organisation et l'exploitation du système d'information ou du fichier, les catégories de données à saisir, la durée de conservation, l'archivage et la destruction des données, l'accès aux données, les autorisations de traitement, la sécurité des données et dans la mesure où des précisions sont nécessaires, les droits des personnes concernées. Avant de procéder à un traitement de données personnelles et notamment de données sensibles ou de profils de la personnalité et de proposer la création d'une base légale, l'organe responsable doit soigneusement examiner si un tel traitement est nécessaire pour accomplir sa tâche légale, quelles finalités il veut atteindre, et en fonction de ces finalités, établir si des données personnelles sont absolument nécessaires et si oui dans quelle mesure (voir aussi 5e Rapport d'activités 1997/98, p. 218ss).

Lors de l'entrée en vigueur de la LPD, plusieurs fichiers contenant des données sensibles ou des profils de la personnalité étaient déjà gérés par les organes fédéraux. Ces fichiers ne reposaient pas tous sur des bases légales suffisantes. Le législateur a tenu compte de cet état de fait et a accordé un délai transitoire de cinq ans pour permettre aux organes fédéraux de se mettre en règle. Au terme de ce délai, qui est arrivé à échéance le 30 juin 1998, les fichiers pour lesquels les bases légales n'avaient pas encore été adaptées, auraient dû être déclarés illicites et cessés d'être utilisés. Dans le cadre de l'examen du message du 17 septembre 1997 concernant la création et l'adaptation des bases légales applicables aux registres des personnes (Modification du code pénal, de la loi fédérale sur la circulation routière et de la loi fédérale sur les Offices centraux de police criminelle de la Confédération; FF 1997 IV 1149, voir aussi p. 206 du présent rapport AT 1.2. et 5ème Rapport d'activités 1997/98, p. 148), le Conseil des Etats s'est rendu compte que les organes fédéraux avaient pris un retard considérable dans l'adaptation des bases légales et que le délai du 30 juin 1998 ne serait pas respecté. Pour éviter l'impasse, le Conseil des Etats a proposé une modification de la LPD prolongeant le délai transitoire de 2 ans. Finalement, l'Assemblée fédérale a adopté, le 26 juin 1998, un arrêté fédéral prolongeant ce délai jusqu'au 31 décembre 2000 (RO 1998 1586). Le Conseil fédéral a chargé les départements de procéder à un inventaire des fichiers contenant des données sensibles ou des profils de la personnalité et ne disposant pas encore de bases légales adéquates. Cet inventaire a été présenté au Conseil fédéral en juin 1998.

La Chancellerie fédérale a été chargée, en collaboration avec les départements concernés, de préparer un message à l'adresse du Parlement regroupant l'ensemble des adaptations légales nécessaires. Ce message concerne les fichiers de contrôle et de gestion des affaires de l'administration fédérale, les fichiers du Département fédéral des affaires étrangères, certains fichiers du Département fédéral de la défense, de la protection de la population et des sports, ainsi que les domaines de la santé, des douanes, des impôts, du personnel, du logement, du service civil et de la chasse. Le Département fédéral de l'intérieur prépare également un message concernant les adaptations légales dans le domaine des assurances sociales (voir aussi p. 260 du présent rapport). Le PFPD collabore aux travaux.

7.3. Liaisons «online» - renforcement de la protection des données

La Commission de gestion du Conseil des Etats a adopté le 17 novembre 1998 une motion invitant le Conseil fédéral à soumettre aux Chambres fédérales une révision de la loi fédérale sur la protection des données. Cette révision doit avoir pour objectif d'imposer des bases légales pour toute liaison «online» même lorsqu'il s'agit d'un projet pilote et de prévoir, pour les requêtes et l'installation de liaisons «online» avec les systèmes informatiques de la Confédération, des normes minimales permettant d'améliorer la collaboration entre la Confédération et les cantons. La Confédération devrait régler l'accès, l'utilisation, la protection et le contrôle de ses banques de données. Tout en reconnaissant la nécessité de modifier la LPD, le Conseil fédéral propose de transformer la motion en postulat. Le PFPD est d'accord avec cette proposition.

Dans le cadre de son inspection des liaisons online dans le domaine de la police (voir p. 229 du présent rapport), la Commission de gestion du Conseil des Etats a adopté une motion demandant au Conseil fédéral de préparer une modification de la LPD ayant pour objectif d'imposer des bases légales pour toute liaison «online» même lorsqu'il s'agit d'un projet pilote. Cette modification devrait également fixer des normes minimales pour les accès des cantons aux systèmes informatiques de la Confédération. Celle-ci devrait régler l'accès, l'utilisation, la protection et le contrôle des banques de données fédérales.

Aux termes de la LPD, les organes fédéraux ne peuvent traiter des données personnelles sans base légale. Si le traitement porte sur des données sensibles ou des profils de la personnalité, celui-ci doit être prévu expressément dans une loi au sens formel. Une base légale expresse est également nécessaire lorsque des

données sont rendues accessibles par procédure d'appel (accès online, principe du self-service). La LPD n'opère pas de distinction entre un traitement appelé à durer ou un traitement effectué à titre d'essai, dans le cadre d'un projet pilote. Cette situation n'est pas sans poser des problèmes en pratique, notamment lorsqu'un projet pilote nécessite le traitement et la communication de données sensibles ou de profils de la personnalité. Un projet pilote doit en principe permettre de tester un système, d'évaluer les nécessités, de préciser l'étendue des données personnelles nécessaires à l'accomplissement des tâches et de déterminer les autorités participant au système ou auxquelles des données doivent être communiquées. Pour ce genre de projet, il n'est guère envisageable de créer une base légale au sens formel avant la fin de la phase de test. Le respect strict de l'exigence d'une base légale au sens formel peut en effet conduire à une réglementation trop large et légitimer des accès non nécessaires et par conséquent affaiblir la protection des données. Il arrive également que pour des raisons d'urgence, certains traitements soient effectués ou certains accès accordés avant que les bases légales ne puissent être mises en place ou parallèlement à leur préparation. Les clauses d'exception aux exigences d'une loi au sens formel pour le traitement de données sensibles ou de profils de la personnalité qui sont prévues à l'article 17, 2e alinéa LPD, ne sont pas adaptées à cette situation. Ainsi, nous sommes amenés à préaviser négativement de tels projets faute de base légale suffisante, même si ces traitements sont conformes aux autres exigences de la protection des données.

Sans remettre en question les exigences de légalité prévues par la LPD, nous sommes ainsi d'avis qu'il convient de prévoir la possibilité de recourir à des projets pilotes et d'autoriser dans certains cas des accès à des systèmes d'information avant que les bases légales ne soient créées. En particulier, nous proposons de modifier la LPD pour permettre la réalisation de projets pilote comme suit:

«Art. 17bis Autorisation de traitement»

1A la demande d'un organe fédéral et après consultation du département concerné ou de la Chancellerie fédérale, le Préposé fédéral à la protection des données peut autoriser le traitement de données sensibles ou de profils de la personnalité avant que les conditions de traitement posées aux articles 17, 2e alinéa et 19, 3e alinéa soient remplies, si:
un motif d'intérêt public important justifie de ne pas retarder la mise en place du traitement; ou
une phase pilote préalable à l'adoption d'une loi au sens formel est indispensable.

2Le préposé peut assortir son autorisation de conditions ou de charges. Il peut en outre la limiter dans le temps et la lier à l'adoption ou à la modification d'une ordonnance du Conseil fédéral.

3La décision du préposé peut être portée par l'organe fédéral requérant ou le département ou la Chancellerie fédérale devant la Commission fédérale de la protection des données. La décision de la Commission n'est pas sujette à recours.»

Cette disposition devrait faire l'objet d'une évaluation cinq ans après son entrée en vigueur.

En ce qui concerne la deuxième partie de la motion de la Commission de gestion du Conseil des Etats, la LPD ne s'applique qu'au traitement de données personnelles effectué par des organes fédéraux ou par des personnes privées. Elle ne s'applique en principe pas au traitement effectué par des organes cantonaux, même si ce traitement se fait dans le cadre de l'exécution de tâches fédérales. Ces traitements sont néanmoins soumis au droit fédéral si les organes cantonaux ne sont pas soumis à des dispositions cantonales de protection des données. En outre, les cantons sont tenus de désigner un organe chargé de veiller au respect de la protection des données.

L'autonomie cantonale en matière de protection des données résulte de l'autonomie organisationnelle cantonale, un principe fondamental du fédéralisme suisse. Du point de vue de la protection des données, la diversité de réglementations qu'elle engendre n'est pas satisfaisante, même si le législateur fédéral a déjà à plusieurs reprises restreint l'autonomie cantonale en matière de protection des données afin d'éviter de trop abaisser le seuil de protection lors de la communication de données aux autorités cantonales. En effet, à l'heure actuelle, seuls 17 cantons disposent d'une loi de protection des données et tous n'ont pas encore mis en place une autorité de protection des données, comme la LPD les y invite. En outre, dans les cantons qui disposent d'une telle autorité, celle-ci a des compétences plus ou moins équivalentes à celle du préposé fédéral. En règle générale, ces autorités n'ont pas l'infrastructure et les moyens suffisants pour accomplir leurs tâches. Avec l'augmentation des échanges de données entre la Confédération et les cantons, notamment des accès par procédure d'appel des autorités cantonales ou communales aux systèmes d'informations de la Confédération, cette situation peut s'avérer problématique en l'absence d'un standard de protection des données suffisant.

Ainsi, nous sommes favorables à ce que le législateur fédéral détermine le standard à respecter en matière d'accès, de traitement, de sécurité et de contrôle des données enregistrées dans des banques de données fédérales et qui sont uti-

lisées par des organes cantonaux ou communaux. En l'absence de dispositions cantonales de protection des données, il conviendrait d'ailleurs de s'interroger sur l'opportunité d'étendre le champ d'application de la LPD, à titre subsidiaire, non seulement aux traitements effectués par des organes cantonaux ou communaux en exécution de tâches fédérales (art. 37 LPD), mais également à tous les traitements effectués par ces organes.

7.4. Droit de recours du Préposé fédéral à la protection des données

Le Conseil fédéral a rejeté une motion de la Conseillère nationale von Felten demandant d'octroyer un droit de recours au Préposé fédéral à la protection des données dans le domaine de la surveillance des organes fédéraux. Appelé à se prononcer sur cette motion, le PFPD a proposé de l'accepter.

Suite à l'arrêt du Tribunal fédéral (ATF 123 II 542) déniant le droit du PFPD de recourir contre une décision d'un Département rejetant une recommandation qu'il a émise (voir 5e rapport d'activités 1997/98, p. 156), la Conseillère nationale von Felten a déposé une motion demandant au Conseil fédéral «de présenter un projet de bases légales octroyant un droit de recours au Préposé fédéral à la protection des données dans le domaine de la surveillance des organes fédéraux.»

Dans sa réponse, le Conseil fédéral propose de rejeter la motion. Il motive en particulier sa proposition par le fait que «bien que le Préposé n'ait pas qualité pour recourir contre la décision d'un département, il n'est pas dépourvu de tout moyen d'action. Il peut en particulier, s'il en va de l'intérêt général, informer le public de ses constatations et de ses recommandations». En outre, «comme le relève le Tribunal fédéral ... les divergences de vues entre autorités relevant d'une seule et même collectivité publique devraient, selon la conception de l'Etat qui prévaut dans notre pays, être aplanies par les autorités politiques dans le cadre de la voie hiérarchique ordinaire et non par la voie de la procédure administrative.»

Appelés à donner notre avis dans le cadre de la procédure de consultation des offices, nous avons proposé d'accepter la motion (voir aussi annexe p. 372). Nous avons en particulier souligné que:
dans l'ordre juridique suisse, il n'est pas exclu qu'une instance judiciaire tranche des conflits entre autorités d'une même collectivité publique. Le PFPD a ainsi un droit de recours contre les décisions de la Commission fédérale d'experts du secret professionnel en matière de recherche médicale. Il peut également requérir des mesures provisionnelles du président de la Commission

fédérale de la protection des données à l'encontre d'un organe fédéral lorsqu'il constate à l'issue d'une enquête que la personne concernée risque de subir un préjudice difficilement réparable.
Le PFPD est un organe spécifique s'acquittant de ses tâches de manière autonome. Il n'est pas soumis à la surveillance d'un département ou de la Chancellerie fédérale. Or, en confiant au département ou à la Chancellerie fédérale le soin de trancher entre le PFPD et un organe fédéral auquel il a adressé une recommandation, le PFPD est soumis à un contrôle de légalité par un organe qui est lui-même soumis à sa surveillance, ce qui est en contradiction avec le statut d'autonomie du PFPD.
La protection des données concerne des biens juridiques élevés et il se justifie de donner la possibilité au PFPD de porter ses recommandations pour décision à une autre instance lorsqu'elles ne sont pas suivies ou qu'elles sont rejetées.
Les personnes concernées ont certes la possibilité de recourir contre les décisions d'un département ou de la Chancellerie fédérale. Cette solution implique toutefois que la personne concernée soit suffisamment orientée sur les violations que le PFPD a recommandé de pallier. Si l'intéressé n'est pas lui-même intervenu dans la procédure, il lui sera particulièrement difficile de faire usage de ses droits. Il n'est en outre pas toujours en mesure d'apprécier si un système d'informations est conforme à la protection des données, notamment du fait de la complexité et de la technicité des systèmes. Le Parlement a d'ailleurs reconnu cette difficulté en accordant au PFPD le droit dans le secteur privé de porter ses recommandations devant la Commission fédérale de la protection des données et le droit de recourir contre les décisions de la Commission d'experts du secret médical en matière de recherche médicale.
En l'absence de recours d'une personne concernée, une recommandation rejetée par l'organe fédéral auquel elle a été adressée et par le département ou la Chancellerie fédérale restera lettre morte, même si une violation des dispositions fédérales de protection des données existe. Les lacunes et les manquements constatés persisteront.
Le système actuel ne permet pas de garantir la sécurité du droit par une pratique uniforme. En accordant au PFPD le droit de porter également ses recommandations à l'égard des organes fédéraux devant la Commission fédérale de la protection des données, on assure une plus grande homogénéité dans l'application du droit et une meilleure sécurité juridique.
Lorsqu'un département ou la Chancellerie fédérale sont impliqués dans un traitement de données personnelles objet d'une recommandation du PFPD, ils se trouvent dans la position de juge et partie.
Le transfert de certaines tâches publiques à des privés, la privatisation de certaines activités et le mélange de certaines tâches légales avec des activités relevant du droit privé, rend la distinction entre organe fédéral et personne privée toujours plus difficile. Une recommandation peut alors concerner à la

fois un organe fédéral et une personne privée, ce qui justifie une procédure identique.
La tendance en Europe et notamment au sein de l'Union européenne (avec la directive 95/46/CE du 24 octobre 1995 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) va vers un renforcement des compétences des autorités chargées de surveiller l'application des dispositions de protection des données. La directive ne fait pas de distinction entre les secteurs public et privé. Elle prévoit en particulier que les organes de protection des données peuvent ester en justice en cas de violation des dispositions de protection des données.

7.5. Application de la loi fédérale sur la protection des données aux procédures administratives de première instance

Les procédures administratives de première instance sont soumises à la loi fédérale sur la protection des données. Seules les procédures administratives contentieuses échappent au champ d'application de la loi.

Cette solution paraît à certains illogique et peut soulever quelques difficultés pratiques, notamment sous l'angle du droit d'accès ou de la communication de données. Toutefois, il s'agit de conflits de compétences positifs. Ceux-ci n'empêchent pas une bonne application du droit et ne perturbent ni l'activité administrative ni la prise de décisions. Nous n'avons à ce jour constaté aucun problème majeur rencontré en pratique par les organes fédéraux du fait du concours de la LPD et de la loi fédérale sur la procédure administrative.

Le législateur était conscient de ces risques de conflits positifs. Il a néanmoins estimé que l'intérêt de la personne concernée devait l'emporter. En effet, «la non-application de la loi sur la protection des données aux procédures administratives de première instance, au sens de la loi sur la procédure administrative, n'aurait pas été sans faire courir de grands risques aux personnes concernées: la plupart des activités administratives auraient été privées de protection des données. La loi sur la procédure administrative régit en effet toutes les causes administratives qui débouchent sur une décision. Du moment que la plupart des activités administratives sont susceptibles d'aboutir à une décision, il eût été très facile aux organes fédéraux d'échapper aux obligations qui leur incombent en vertu de la protection des données.» (FF 1988 II 451)

On est en droit de se demander si l'exclusion des procédures pendantes du champ d'application de la LPD est une solution adéquate et s'il ne faudrait pas

soumettre ces procédures à la LPD, - pour le moins à la surveillance du PFPD – quitte à prévoir certaines dispositions spécifiques dérogeant à la LPD.

7.6. Instance de recours en cas de décisions concernant la protection des données

En cas de litige grave relevant de la loi sur la protection des données, il convient d'indiquer aussi la possibilité de faire appel à la Commission fédérale de la protection des données indépendamment de l'indication des voies de droit ordinaires.

L'Office fédéral du développement économique et de l'emploi (OFDE) nous a demandé si la Commission fédérale de la protection des données était également compétente dans les procédures de recours portée devant des autorités de recours relevant du droit de l'assurance-chômage lorsque le différend concernait la protection des données. La question se pose d'une manière générale pour d'autres organes de la Confédération qui engagent plaintes et recours en rapport avec la protection des données devant les commissions de recours de leur département. Nous avons transmis les questions à la Commission fédérale de la protection des données (CFPD). Nous avons résumé ci-dessous sa réponse.

Lors de la promulgation de la LPD en 1992, le législateur fédéral a voulu que les questions litigieuses avec les organes fédéraux sur l'application des dispositions fédérales de protection des données relevant du droit public ne soient pas tranchées dans le cadre des procédures de recours spécifiques à chaque domaine, mais que ces différends, puisqu'ils relèvent du droit de la protection des données, soient portés devant la CFPD et que les décisions de cette dernière dans tous les domaines du droit administratif fédéral puissent faire l'objet d'un recours de droit administratif devant le Tribunal fédéral. C'est ce qu'il ressort de l'art. 25, 5^{e} al. LPD et de l'art. 100, 2^{e} al., lettre a de la loi fédérale d'organisation judiciaire (OJ). Seules les règles légales spéciales expresses telles que les connaît actuellement (uniquement) la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure demeurent réservées. La promulgation de la LPD n'a pas donné lieu à d'importantes révisions du droit administratif fédéral, ni en ce qui concerne les prescriptions matérielles de protection des données, ni quant à la protection juridique. L'annexe à la LPD (modifications de lois fédérales) a uniquement permis d'introduire un très petit nombre de normes matérielles centrales dans d'autres lois fédérales. Ce n'est que maintenant, donc ultérieurement, que les dispositions de procédure seront ponctuellement modifiées. On comprend parfaitement qu'en 1992, le législateur n'ait pas procédé à une révision générale des prescriptions en matière de droit

matériel ou de procédure. En effet, en tant que matière touchant tous les domaines juridiques, le droit de la protection des données influe sur de très nombreuses règles du droit administratif fédéral. Par ailleurs, seule la pratique permet de déterminer ce qui constitue une question litigieuse majeure ou non en matière de droit de la protection des données. En application de la LPD et d'autres prescriptions de droit fédéral en matière de protection des données, les organes fédéraux sont régulièrement appelés à trancher des différends portant sur l'interprétation des normes. Dans l'ATF 123 II 534, le Tribunal fédéral s'est exprimé ainsi à propos du conflit entre la loi sur la protection des données et la loi sur l'assurance-accidents: «La loi sur la protection des données et l'ordonnance sur la protection des données sont plus récentes que la loi sur l'assurance-accidents et l'ordonnance sur l'assurance-accidents. Un texte législatif plus récent a la préséance sur un texte plus ancien même si ce dernier n'a pas été abrogé ou révisé formellement (lex posterior derogat legi priori). Le fait que lors de la promulgation de la loi sur la protection des données, les dispositions de la loi sur l'assurance-accidents et de l'ordonnance sur l'assurance-accidents relatives à la consultation des dossiers n'aient pas été modifiées ne justifie pas la préséance des normes légales de l'assurance-accidents.» Le Tribunal fédéral ajoute: «Des questions juridiques touchant la protection des données peuvent se poser à l'intérieur d'une procédure déterminée dont l'objet essentiel est tout autre, par exemple le droit des assurances sociales. Dans ce cas, les aspects du droit de la protection des données et les questions réglées par une loi spéciale seront appréciés ensemble dans le cadre des procédures correspondantes (...). Néanmoins ils peuvent être aussi abordés comme objet autonome, indépendamment d'une autre procédure, et peuvent dans ce cas faire l'objet d'une procédure devant de la Commission fédérale de la protection des données qui rendra une décision susceptible d'un recours de droit administratif devant le Tribunal fédéral". Néanmoins, en vertu des règles figurant aux art. 25 et 33 LPD, il est clair que des dispositions spécifiques de protection des données peuvent aussi être consignées par exemple dans le droit des assurances sociales et que les différends survenant à ce propos dans la procédure spéciale doivent être tranchés en vertu de la LPD et de l'OJ. En se basant sur les art. 17 ss LPD, il est clair que la LPD doit être complétée par des normes pertinentes en matière de protection des données en fonction de chaque domaine spécifique. En cas de question litigieuse majeure touchant le droit de la protection des données, il convient de modifier l'indication des voies de droit et de mentionner la CFPD. Cette indication spéciale des voies de droit doit avoir lieu dans tous les cas où il est clair qu'il s'agit d'une question litigieuse de protection des données d'importance majeure. Dans le domaine d'application de l'assurance-chômage, ce genre de questions litigieuses capitales portent par exemple sur des renseignements touchant la protection de la personnalité et émanant des organes d'assurance-chômage dans la mesure où ils sont admis en vertu de l'art. 97, 2^{e} al. LACI, ou bien des demandes de renseignements d'une personne assurée en

vertu de l'art. 126, 2e al. OACI et de l'art. 8 LPD. Il s'impose alors de modifier l'indication des voies de droit pour les motifs suivants: tout d'abord, comme nous l'avons déjà mentionné, outre l'art. 101 LACI, nous trouvons sur un pied d'égalité l'indication des voies de droit des art. 25 et 33 LPD; en outre, le devoir d'indiquer les voies de recours de l'art. 35 PA s'entend comme une véritable indication des voies de recours. Si une autorité indique en connaissance de cause une voie de recours erronée, elle contrevient au principe de la bonne foi. Si, selon la jurisprudence du Tribunal fédéral, une partie ne peut obtenir gain de cause en raison d'une indication inexacte des voies de droit, mais contrevient manifestement à la bonne foi si elle connaît l'inexactitude des voies de droit indiquées ou si elle aurait dû la reconnaître en y apportant l'attention nécessaire (ATF 121 II 278), une autorité ne commet une infraction au droit que si elle indique manifestement des voies de droit erronées. Demeurent néanmoins réservées, ainsi que nous l'avons déjà mentionné, les cas où il n'est absolument pas évident que l'on se trouve en présence d'une question litigieuse relevant purement de la protection des données et d'importance majeure.

8. Protection et sécurité des données

8.1. La révision de l'ordonnance sur le système de gestion du personnel de l'armée (PISA) et l'application des exigences en matière de protection et de sécurité des données.

Fin 1996, le projet «PISA-Security» et au milieu de l'année 1997 la révision de l'ordonnance sur les contrôles militaires (OC- PISA) dans le groupe du personnel de l'armée furent mis en route. Parmi les raisons importantes de cette révision on comptait alors des questions relatives aux domaines techniques ainsi qu'à la protection des données (de même que des aspects de qualité et de sécurité des données). Le maître de fichier assuma la responsabilité qui lui avait été conférée par le Parlement et instaura les organisations de projet nécessaires.

Le système de gestion du personnel de l'armée (PISA) présente à ce jour les mesures de sécurité ci-dessous, adéquates et suffisantes pour le traitement de données sensibles ainsi que de profils de la personnalité:

- procédé de chiffrage symétrique avec une longueur de clé de 112 bits au moins;

- l’identification et l’authentification ne se fait pas seulement par l’introduction de l’identification de l’utilisateur et d’un mot de passe, mais utilise en plus un procédé du type «Challenge/Response». Ce procédé est basé sur l'utilisation d'une petite calculette (Access Token) lié à un mot de passe pour utiliser la calculette. Il se base en plus sur la génération de chiffres aléatoires qui rendent pratiquement impossible (probabilité minime) un accès non autorisé au système;
- journalisation des activités attenant à la sécurité;
- autorisation d'accès uniquement lorsque ceci est nécessaire pour l'accomplissement de la tâche.

Quelques rares unités de la Confédération et des cantons qui ont pu mettre en service le système PISA n'ont pas pu appliquer à temps les mesures de sécurité imposées bien qu'elles aient été informées à temps par le groupe du personnel de l'armée. Un délai reporté a donc été convenu avec ces unités afin qu'elles puissent quand même mettre en route les mesures de sécurité nécessaires.
Nous avons – dans la mesure du possible – accompagné la révision de l'ordonnance afin de mieux comprendre l'intégralité du système de contrôle de l'armée. Ce sont souvent des «informations informelles» surgissant dans des discussions et souvent non documentées ou inconnues de personnes extérieures au groupe qui ont largement facilité la compréhension. Nous avons de cette manière réussi à proposer des solutions conformes aux exigences de la protection des données, solutions qui ont dans maints cas été intégrées dans l'ordonnance révisée. Pourtant, nous n'avons pas pu comprendre les arguments suivants du DDPS:
en relation avec l'origine des données on utilise le terme de tiers. D'un point de vue de la protection des données ainsi que par souci de transparence, nous avons demandé que l'on fournisse une description ou une énumération complète de ce qu'est un tiers. Malheureusement, nos suggestions n'ont pas été retenues ce qui fait que l'origine des données est encore toujours formulée de manière trop imprécise.
En ce qui concerne la conservation pour un durée limitée et la communication des données conservées, nous avons rendu attentif au fait que le volume des données est bien trop important pour les buts idéals et non commerciaux (environ 43 champs de données, y compris l'état de service qui contient des données sensibles). Malheureusement, nous n'avons dans ce cas pas non plus réussi à nous faire entendre suffisamment.

8.2. L'anonymisation de données personnelles à l'aide de procédés de chiffrage pour la statistique de l'aide sociale

Dans le cadre de la statistique sur l'aide sociale, les données sont saisies dans les communes puis transmises à l'Office fédéral de la statistique (OFS) pour y être traitées. Du point de vue de la protection des données ces données doivent être anonymisées aussi rapidement que possible, à savoir dès que le but du traitement le permet. Ceci dans le but que l'on ne puisse plus identifier les personnes individuelles, sauf aux endroits où les données ont été saisies (et où elles sont de toute façon connues). Ces exigences peuvent être remplies par l'utilisation de procédés de chiffrage, sans que ceci entrave le traitement des données à des fins statistiques.

L'OFS met à disposition des communes un système qui permet de saisir sous forme électronique les données nécessaires à la statistique sur l'aide sociale. Pour des raisons de maintien du secret, les données doivent être chiffrées lors de leur transmission à l'OFS. On utilise pour cela aussi bien un procédé de chiffrage asymétrique qu'un procédé symétrique; le procédé symétrique pour le chiffrage des données et l'asymétrique pour le chiffrage des clés symétriques.
Un procédé de chiffrage asymétrique est caractérisé par le fait que des clés différentes sont utilisées pour le chiffrage et le déchiffrage. La clé de chiffrage (clé publique) permet par exemple seulement de chiffrer les données, mais pas de les déchiffrer (une clé secrète privée étant nécessaire pour cela). La clé publique est accessible à toutes les personnes impliquées dans le système. Lors de la transmission de données à un destinataire, celles-ci doivent être codées avec la clé publique du destinataire. Ce dernier est alors en mesure de déchiffrer les données avec sa clé privée (secrète).
Un procédé de chiffrage symétrique est caractérisé par le fait qu'il utilise une seule clé aussi bien pour le chiffrage que pour le déchiffrage et que la puissance de calcul nécessaire pour le chiffrage est bien inférieure à ce qu'elle est pour les procédés asymétriques.
Dans le projet dont il est question, les données sont regroupées en données identifiantes (nom, prénom, rue, ...) et données utiles (données qui n'identifient pas les personnes). Les données utiles sont en fait les données qui intéressent pour la statistique. L'utilisateur – en l'occurrence l'OFS – génère deux paires de clés (clés de chiffrage et de déchiffrage asymétrique), étant donné que les données d'identification et les données utiles doivent être chiffrées différemment. L'OFS communique les deux clés de chiffrage (clés publiques) à chaque organe chargé de faire des saisies et conserve en ses mains les deux clés de déchiffrage (clés privées).
Les organes de saisie procèdent alors au chiffrage des données en utilisant l'algorithme symétrique performant IDEA, avec des clés distinctes pour les

données d'identification et les données utiles. Ensuite, ils procèdent au chiffrage des deux clés symétriques générées en utilisant une des deux clés asymétriques afin de pouvoir transmettre les données de manière sécurisée (y compris les clés symétriques) à l'OFS. L'OFS est alors en mesure de déchiffrer les deux clés symétriques transmises en utilisant les deux clés privées asymétriques, puis de déchiffrer les données à l'aide de ces deux clés. Ensuite, les données d'identification sont chiffrées à l'aide du procédé symétrique, c.-à-d. anonymisées avant d'être stockées dans la base de données commune qui regroupe toutes les données qui ont été saisies. Pour des raisons de sécurité, ce processus doit avoir lieu aussi rapidement que possible afin d'éviter que des données identifiantes soient présentes dans le système sous forme non codée.
La solution repose sur la confiance que l'on accorde à une instance ou à une personne. L'OFS sera en possession de clés qui lui permettent de déchiffrer les données précédemment anonymisées, donc de rompre l'anonymat. Nous avons informé l'OFS que nous saluons sa démarche dans ce projet. Nous avons en outre attiré son attention sur le fait qu'une éventuelle annulation de l'anonymisation ne devait avoir lieu que dans le cadre d'une procédure bien contrôlée au sein de l'OFS. En particulier, il y a lieu de consigner le but de la désanonymisation. D'autre part, il faut veiller à ce que la clé ne puisse être utilisée que conformément au principe des quatre yeux (séparation des fonctions) et que de tels processus sensibles soient journalisés.

8.3. Etat de l'application des mesures de sécurité dans le système SiRück (comptes des prestations de sécurité des requérants d'asile)

En janvier 1995, le Préposé fédéral à la protection des données a émis une recommandation (voir 2e rapport d'activités 1994/95 page 270 et 3e rapport d'activités 1995/96 page 150) concernant l'application insuffisante des dispositions de protection des données dans le système SiRück. La séance finale pour l'application des mesures de protection des données que nous avons demandées n'aura lieu que dans la deuxième moitié de 1999, c'est-à-dire près de 4 ans après que nous ayons émis notre recommandation.

Dans sa recommandation, le PFPD avait proposé d'utiliser des procédés de chiffrage pour l'application des mesures de sécurité des données. La Section Sécurité informatique de l'Office fédéral de l'informatique (OFI) avait été chargée à l'époque d'étudier quelles étaient les possibilités de chiffrage pour le système SiRück. L'expertise disait alors ceci:
un passage direct à un procédé de chiffrage de bout en bout n'est pas possible car une telle solution exigerait une nouvelle conception de l'application SiRück.

Il faudrait alors mettre en place un environnement client-serveur et non seulement une émulation de terminal VT pour le traitement des données. Il était difficile à l'époque d'évaluer les efforts, aussi bien en temps qu'en argent, étant donné que ceux-ci dépendaient fortement du type de mise en œuvre choisi. Ce qu'on pouvait cependant dire à coup sûr à l'époque, c'est qu'une migration ne pouvait pas avoir lieu en l'espace d'une année. On indiqua néanmoins des projets de solution concrets.
Par la suite, on a dû constater que les unités participant au système avaient en partie des avis divergents en ce qui concerne les mesures de sécurité des données. On a dû d'ailleurs constater par la suite que les unités s'étaient laissées conseiller par différentes sociétés conseil en matière de sécurité, ce qui fit encore une fois perdre du temps en ce qui concerne la planification et la réalisation des mesures de sécurité. Dans les projets, nous devons constater de manière répétée que les mandants (maîtres de fichier/organes responsables) ne définissent pas de manière assez exacte les exigences envers un traitement des données effectué par des tiers (outsourcing). Il y a lieu de stipuler de manière aussi précise que possible dans une base légale ou dans le contrat quelles sont les exigences que le contractant (tiers) doit remplir.
Après avoir à maintes reprises reporté la date, la séance finale relative aux mesures de sécurité qui ont été appliquées devrait définitivement avoir lieu dans le courant du premier semestre 1999. Il est alors prévu que le système sera basé sur une technique World Wide Web et une architecture client-serveur. Ce n'est qu'à cette date que la variante de chiffrage définitive devrait être mise en œuvre.

8.4. Etat des travaux de mise en œuvre des exigences de protection et de sécurité des données auprès du système de gestion du personnel PISEDI

La recommandation du Préposé fédéral à la protection des données de mai 1997 (voir 5e rapport d'activités 1997/98, pages 130 ss) concernant l'application insuffisante des dispositions de protection et de sécurité des données dans le domaine du système de gestion du personnel PISEDI a fait que l'organe responsable a élaboré un règlement de traitement avec l'assistance du PFPD. Il est prévu que ce règlement servira de modèle pour d'autres règlements de traitement. D'autre part, dans le domaine de la sécurité des données, on est en train d'étudier le catalogue des mesures basé sur la directive de sécurité DS S02. Finalement, les mesures de sécurité encore manquantes seront appliquées au sein du système.

Le système de gestion du personnel PISEDI peut être divisé en deux domaines de fonctions principaux: la partie «postulant» et la partie «collaborateur». Si un postulant est engagé, les données «postulant» sont transférées dans la partie «collaborateur»; si le postulant n'est pas engagé, on lui renvoie son dossier et l'on supprime les données dans le système informatique après une certaine période. D'autre part, le système informatique informe le service du personnel d'événements tels que anniversaires, promotions, échéance des temps d'essais, échéances pour appréciations, anniversaires de service, etc. Le système informatique permet également de générer des états tels qu'un aperçu des données du postulant, des rapports relatifs à un collaborateur tels que le plan des postes, les communications mensuelles à l'Office fédéral du personnel, des listes de quotas, etc.
En collaboration avec le maître de fichiers et le responsable informatique, nous avons documenté et discuté le processus du traitement des données relatives au personnel du Secrétariat général du DFI. A cette occasion, nous avons réalisé que les certificats de travail n'étaient pas établis par le système PISEDI, mais qu'ils étaient rédigés à l'aide du système de traitement de texte Word.
Nous avons demandé une énumération exhaustive aussi bien pour l'origine que pour la communication des données. Il doit être clairement visible auprès de quels organes les données sont saisies et à qui elles sont communiquées. La description de ces organes doit être précise et limitative. Le maître de fichiers défend le point de vue qu'une énumération exhaustive n'est pas possible.
Dans le domaine des procédures de contrôle nous avons jusqu'à ce jour rendu attentif aux aspects suivants:

- dépouillement des journaux;
- contrôle des données saisies dans les champs à texte libre;
- vérification si les données dont on n'a plus besoin sont supprimées;
- surveillance des procédés de modification (gestion des utilisateurs ainsi que modifications apportées au système telles que changements au niveau du matériel, des logiciels et des fonctionnalités);
- implication de l'organe de surveillance lors de consultations du type Query (permettant des consultations libres).

Nous avons dû constater que le système était largement ouvert en ce qui concerne la manière d'accéder à la base de données et les possibilités d'accès offertes. Il était possible à chaque utilisateur (entre-temps cette fonction a été restreinte à l'administrateur système) de faire une consultation du type Query (avec des possibilités de recherche non restreintes); d'autre part une recherche peut être effectuée sur n'importe quel champ de données. C'est le produit utilisé qui en soi offre toutes ces possibilités très larges et la question se pose comment on peut restreindre ces fonctions de recherche. Grâce à l'utilisation du gestion-

naire d'événements et de la fonction Query, de telles possibilités de recherche ne sont à notre connaissance pas nécessaires.
Le système permet de journaliser les modifications, mais pas les consultations. Un tel module devrait être développé séparément. Il n'est donc pas possible a posteriori de constater qui a consulté quelles données dans quel but.
En ce qui concerne le règlement de traitement, la question du concept de sécurité est encore toujours en suspens. Dans ce contexte, la question se pose de savoir quelles modifications doivent être journalisées et comment les moyens informatiques sont à configurer. Il est prévu de fournir les données manquantes au PFPD d'ici le premier trimestre 1999, après quoi les points en suspens du règlement de traitement seront discutés au sein du PFPD ainsi qu'au Secrétariat général du DFI et un règlement modèle sera élaboré qui devrait servir de base à d'autres règlements de traitement. Finalement, les mesures nécessaires devront être appliquées dans le système de gestion du personnel.

9. Divers

9.1. Base de données pour enfants avec domicile inconnu – protection des données en Belgique

Suite à un postulat en rapport avec le problème au niveau international des enfants qui ont été enlevés ou dont on a abusé, nous avions à étudier la question si des réserves devaient être émises du point de vue de la protection des données si une succursale d'un organisme belge s'occupant de rechercher des enfants dont le domicile est inconnu exploite en Suisse une banque de données .

Le postulat Simon (97.3322) traite du problème à l'échelle internationale des enfants qui ont été enlevés ou dont on a abusé. Dans ce cadre, nous avions à étudier la question si des réserves devaient être émises du point de vue de la protection des données à l'encontre d'une banque de données exploitée en Suisse par une succursale d'un organisme belge s'occupant de rechercher des enfants dont le domicile est inconnu.
Le but de cette banque de données est d'échanger au moins avec la maison mère de l'organisation des informations concernant des enfants portés disparus ou dont on a abusés sexuellement. Il s'agit là d'une communication de données personnelles à l'étranger. Conformément à la LPD, des données personnelles ne peuvent être communiquées à l'étranger que si ceci ne porte pas une grave atteinte à la personnalité des personnes concernées. Ceci est notamment le cas si

le pays destinataire ne dispose pas d'une protection des données équivalente à la nôtre. La législation en matière de protection des données belge est comparable à celle de la Suisse. Il n'y a donc rien qui s'oppose à une telle communication de données vers la Belgique. Nous avons cependant attiré l'attention sur le fait que la succursale en Suisse doit respecter les principes généraux de la LPD (licéité de la collecte, proportionnalité, finalité, exactitude, sécurité des données, garantie du droit d'accès). Le principe de la sécurité des données a pour conséquence que la succursale doit, notamment dans le domaine de la transmission des données à d'autres succursales européennes ou à la maison mère, en particulier par le biais d'une liaison électronique, prendre des mesures techniques et organisationnelles conformes à la LPD et l'OLPD. Ces mesures servent notamment aux buts liés au contrôle de l'accès, des données personnelles, des supports de données, du transport, de la communication, de la conservation, des utilisateurs et de la saisie.

9.2. Commercialisation d'un CD-ROM concernant des données relatives aux détenteurs de véhicules à moteur

Dans sa décision du 18 mars 1998, la Commission fédérale de la protection des données a ordonné la cessation définitive de la production et de la diffusion du CD-Rom AUTOdex (cf. 5^{e} Rapport d'activités, p. 237). Nous avons constaté ultérieurement que le CD-ROM en question était à nouveau disponible sur le marché. Le 31 août 1998, nous avons demandé à la Commission fédérale de la protection des données de rendre une décision exécutoire.

Dans sa décision du 18 mars 1998, la Commission fédérale de la protection des données a ordonné que cessent la production et la diffusion du CD-ROM AUTOdex contenant les données relatives aux détenteurs de véhicules à moteur en Suisse. Le 22 juillet 1998, l'entreprise responsable a annoncé le CD-ROM en question comme fichier auprès de nos services. Au cours des jours qui ont suivi, nous avons constaté que la diffusion d'une nouvelle version du CD-ROM était à nouveau en vente sur le marché. L'Association des services des automobiles que nous avons consultée nous a confirmé que depuis la décision rendue par la Commission fédérale de la protection des données, aucun canton n'avait octroyé l'autorisation de produire le CD-ROM, à la suite de quoi nous avons prié la Commission fédérale de la protection des données de rendre une décision exécutoire. Nous demandions en substance la saisie du bénéfice réalisé après la décision de la Commission fédérale de la protection des données, ainsi que la menace de peine pour insoumission selon l'art. 292 CP. Au cours de l'échange de correspondance, l'entreprise en question a défendu pour l'essentiel le point de

vue selon lequel le nouveau CD-ROM en vente ne constituait pas une nouvelle version du CD-ROM précédent, mais une version différente aux possibilités de recherches restreintes. Elle estimait en outre qu'en agissant ainsi, elle n'avait pas contrevenu à la décision de la Commission fédérale de la protection des données et qu'en outre, il n'y avait pas matière à exécution. Par ailleurs, elle considérait que la demande de saisie du bénéfice constituait une atteinte au droit constitutionnel à la liberté de propriété. Nous avons estimé que le CD-ROM en question n'était pas une version entièrement différente, mais la quatrième version du CD-ROM déjà connu. A notre avis, la production et la diffusion de cette quatrième version du CD-ROM constituaient un cas d'inobservation de la décision de la Commission fédérale de la protection des données. Au surplus, nous avons précisé que l'entreprise en question ne pouvait invoquer la liberté de propriété étant donné qu'elle n'était pas propriétaire des données concernant les véhicules. Nous attendons actuellement la décision de la Commission fédérale de la protection des données.

9.3. Enregistrements vidéo et thérapies

La relation thérapeute-patient institue un rapport de confiance de type particulier. Celui qui envisage d'enregistrer par caméra vidéo les entretiens avec des patients doit pouvoir s'appuyer sur un motif justificatif. Pour des enregistrements vidéo, ce motif résulte principalement du consentement de la personne enregistrée, celui-ci devant être obtenu avant de procéder aux enregistrements. En cas de refus, les enregistrements sont interdits. Les personnes qui ont été enregistrées peuvent en tout temps demander que les données les concernant soient effacées.

Un couple s'est rendu chez une conseillère conjugale. Après vingt minutes d'entretien, il s'est aperçu que la conversation était enregistrée à son insu par système vidéo. Il a instantanément demandé l'interruption de l'enregistrement et exigé la destruction des données qui avaient déjà été enregistrées. La thérapeute a refusé d'effacer les données et l'entretien en est resté là. Le couple s'est adressé à nos services pour savoir à quel moment il aurait dû être informé de l'enregistrement, si un enregistrement de ce type suppose un consentement préalable, s'il peut maintenir sa requête en vue d'une destruction des données et comment s'y prendre.
Les enregistrements vidéo constituent des données personnelles au sens de la LPD. Les propos échangés dans le cadre de psychothérapies contiennent des informations sur la santé et la sphère intime et, à ce titre, sont considérés comme des données sensibles. En vertu des principes généraux de la LPD, les collectes

de données personnelles doivent toujours se faire de manière licite et leur traitement doit s'effectuer conformément aux principes de la bonne foi et de la proportionnalité. Par conséquent, il est interdit de rassembler des données à l'aide de techniques auxquelles la personne concernée ne s'attend pas et avec lesquelles elle n'aurait pas été d'accord. En l'occurrence, il y a lieu de traiter autant de données qu'il est nécessaire, mais aussi peu que possible. En outre, les données personnelles ne peuvent être traitées que dans le but qui est indiqué lors de leur collecte (p. ex: à des fins de formation), qui est prévu par une loi ou qui ressort des circonstances.
Celui qui entend traiter des données personnelles doit en principe se prévaloir d'un motif justificatif. Pour les enregistrements vidéo effectués dans le cadre d'une thérapie de couple, le motif justificatif réside dans le consentement préalable exprès de toutes les parties concernées. Si une personne s'oppose à un enregistrement vidéo, l'utilisation de cette technique est tout simplement interdite. Dans tous les cas, les patients doivent être informés au préalable et de manière circonstanciée de l'enregistrement prévu (principe de transparence). Cette manière de procéder constitue aussi un point essentiel en raison du rapport de confiance particulier qui existe entre la personne qui vient chercher aide et conseil et le thérapeute. En outre, toute personne concernée peut demander à n'importe quel moment une interruption des enregistrements et la destruction des enregistrements précédents. Les thérapeutes ont l'obligation de respecter ces demandes. Dans le cas précis, nos services ont attiré l'attention de la thérapeute sur l'obligation qui lui était faite et celle-ci a détruit les données en sa possession.

9.4. Le préposé fédéral à la protection des données n'est pas un organisme de certification.

De nombreuses entreprises s'adressent à nous pour savoir si leurs conditions générales, clauses de consentement ou encore les enveloppes qu'elles utilisent sont conformes aux principes de la protection des données. Nous avons coutume de leur répondre qu'en leur qualité de maîtres de fichiers, ils assument la responsabilité pleine et entière du traitement des données. Si nous conseillons les particuliers dans le domaine de la protection des données, nous n'avons en revanche aucune compétence en matière de certification.

Souvent des entreprises nous demandent si leurs conditions générales et clauses de consentement correspondent aux exigences de la LPD. Elles formulent fréquemment aussi le souhait de pouvoir mentionner notre nom sur leurs documents, comme gage d'un traitement des données conforme aux dispositions de la loi. Il arrive par ailleurs régulièrement que des imprimeries nous invitent à

vérifier l'opacité de leurs enveloppes destinées au trafic postal ou bancaire et à en attester la qualité.
Comme nous avons déjà eu l'occasion de le répéter à plusieurs reprises, le PFPD n'a pas la faculté de délivrer une attestation de conformité en rapport avec les traitements de données. Nous précisons à cet endroit que, pour des impératifs de capacité, il ne donnera plus suite à de telles requêtes. Les maîtres de fichiers sont personnellement responsables d'un traitement des données personnelles conforme à la loi. A cet effet, nous leur indiquons les possibilités de contrôle existantes. En ce qui concerne en particulier les enveloppes, nous avons l'habitude de dire qu'il faut s'assurer de leur opacité en les exposant, munies de leur contenu, à une source de lumière (p. ex.: lampe de bureau ou lampe de poche), comme pourrait le faire abusivement un tiers non autorisé. Ce procédé permet de constater rapidement si le contenu d'une enveloppe peut ou non être lu en transparence et dans quelle mesure la protection est effectivement assurée lors de l'acheminement du courrier. Dans des cas d'espèce, les dispositions de l'OLPD également applicables.

9.5. Protection des données et publication de livres

En relation avec la publication d'un ouvrage à contenu politique, le Préposé fédéral à la protection des données a été amené à dire dans quelle mesure les auteurs de livres pouvaient être mis au bénéfice des dispositions aménagées spécialement pour les médias en matière de restriction du droit d'accès.

Dans un Etat de droit, les médias sont investis d'une mission particulièrement importante. Ils informent sur les visions du monde et les pensées politiques les plus variées permettant ainsi à la population de se forger librement une opinion. Pour que les médias puissent tenir leur rôle, il faut naturellement qu'ils bénéficient d'une certaine liberté d'action dans le domaine du traitement des données personnelles.
L'article 10 de la LPD répond à ce besoin en aménageant à l'intention des journalistes employés par un média à caractère périodique (journalistes indépendants inclus) la possibilité de refuser, de restreindre, voire de différer le droit d'accès (art. 8 LPD) à des données personnelles dans la mesure où cette information fournit des indications sur leurs sources, donne lieu à un droit de regard sur des projets de publication ou compromet la libre formation de l'opinion publique. Cela signifie donc que le particulier ne saurait invoquer un droit à la protection de sa personnalité lorsque la libre formation de l'opinion publique présente un intérêt supérieur. L'appréciation de chaque cas s'effectue,

comme pour tout autre traitement de données, à la lumière des principes énoncés aux articles 4 et suivants de la LPD.
Si les livres et les films contribuent indéniablement à la libre formation de l'opinion publique, force est de constater qu'ils n'ont pas le même impact sur le public. Cela s'explique par le fait que des médias comme les journaux, la radio ou la télévision, qui diffusent leurs informations avec une certaine régularité, pèsent d'un poids nettement plus lourd dans la formation de l'opinion d'un public nettement plus important. Vouloir mettre la publication de livres et de films au bénéfice de la réglementation spéciale de l'article 10 LPD serait donc en contradiction avec le principe de proportionnalité, notamment du fait que les maîtres de fichiers accusés d'atteinte illicite à la personnalité seraient alors presque toujours incités à déclarer qu'ils récoltent des données dans l'optique d'une publication (voir à ce propos FF 1998 II 468). Par conséquent, seules sont applicables à la publication de livres et de films les dispositions générales de la restriction du droit d'accès (art. 9 LPD), ce qui n'est tout de même pas négligeable. En vertu de cet article, un maître de fichier privé peut, en particulier, refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi, dans la mesure où ses intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à des tiers.
Dans la pratique, il n'est pas toujours aisé de dire laquelle des deux dispositions s'applique. C'est le cas notamment lorsqu'un journaliste indépendant travaille à la fois pour un média à caractère périodique et à la rédaction d'un livre. Dans la mesure où il utilise les mêmes archives pour ses deux activités, il incombera au juge compétent, en cas de procès, de rendre un jugement adéquat, compte tenu de tous les éléments en présence.

III. ACTIVITES INTERNATIONALES

1. Conseil de l'Europe

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a tenu sa 14e réunion du 2 au 4 septembre 1998. Il a en particulier adopté un amendement à la Convention devant permettre aux Communautés européennes d'y adhérer. Cet amendement doit être approuvé par le Comité des Ministres dans le courant 1999. Le T-PD a également modifié son règlement interne afin de préserver le droit des minorités lors des votes sur des questions relevant de la compétence communautaire. Il a commencé l'examen d'un protocole additionnel à la Convention. Ce dernier prévoira l'obligation pour les Etats contractants d'instituer des autorités de contrôle agissant de manière indépendante pour surveiller le respect des dispositions de protection des données. Ces autorités devraient se voir reconnaître le droit d'ester en justice, ou au moins de porter à la connaissance des autorités judiciaires les violations constatées dans le domaine de la protection des données. Ce protocole régira aussi les flux transfrontières de données vers des Etats non contractants. Enfin, le T-PD a convenu de poursuivre ses travaux dans le domaine des clauses contractuelles lors de flux transfrontières de données.

Le Groupe de projet sur la protection des données (CJPD) s'est réuni à deux reprises. Il a terminé l'examen du projet de recommandation sur la protection de la vie privée dans l'Internet et des lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel dans les inforoutes. Ces deux textes ont été adoptés par le Comité des Ministres le 23 février 1999 et peuvent être consultés sur Internet (http://www.coe.fr/dataprotection). Les lignes directrices s'adressent aux utilisateurs d'Internet et aux fournisseurs de service. Elles rappellent leurs droits et obligations, et elles recommandent certains comportements ou mesures à prendre pour assurer le respect de la vie privée. Le CJPD a également adopté un rapport sur l'évaluation de la pertinence de la Recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Dans ce rapport, le CJPD propose en particulier d'examiner la nécessité d'adopter un instrument juridique complémentaire à cette recommandation pour tenir compte des pratiques policières et judiciaires actuelles dans la lutte contre la criminalité. Le groupe de projet s'est d'autre part prononcé en faveur de l'introduction de dispositions de protection des données dans le projet de convention sur la criminalité dans le cyberespace. Il a finalement poursuivi ses

travaux en vue de l'adoption d'une recommandation sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

2. Relations avec l'Union européenne

La Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, 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 (http://www.europa.eu.int/comm/dg15/fr/index.htm) est entrée en vigueur le 25 octobre 1998. A cette date, les 15 Etats membres de l'Union européenne devaient avoir transposé la directive dans leur droit interne. Toutefois, seuls cinq Etats (Italie, Grèce, Portugal, Suède et Royaume-Uni) ont été en mesure de respecter ce délai. Depuis lors, la Belgique a adopté une nouvelle loi. Le 25 octobre 1998 est également entrée en vigueur 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.

L'objectif de la Directive européenne 95/46CE est d'assurer un haut niveau de protection de la vie privée des citoyens dans tous les Etats membres, tout en permettant la libre circulation des données personnelles à l'intérieur de l'Union européenne et de supprimer ainsi les distorsions de concurrence et les risques de délocalisation. La directive couvre le traitement de données personnelles dans les secteurs public et privé dans la mesure où ces traitements entrent dans le champ de compétence de l'Union européenne. Ainsi, la directive ne s'applique pas aux traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'Etat. La directive stipule les conditions dans lesquelles un traitement automatisé ou non automatisé de données personnelles est légitime. Elle énonce les droits de la personne concernée (droits d'information, d'accès, de rectification, de s'opposer au traitement et de recours). Elle règle les qualités que doivent avoir les données et leur traitement (exactitude, collecte loyale et licite, finalité légitime et licite, compatibilité, proportionnalité, confidentialité, sécurité et notification). En matière de surveillance, une autorité de contrôle indépendante avec pouvoir de décision et droit d'ester en justice est prévue. La directive abandonne la référence au fichier, sauf pour les données manuelles, pour se concentrer sur les traitements. Enfin, elle règle les flux transfrontières de données. Ceux-ci doivent être libres au sein de l'Union européenne. Ils sont par contre en principe interdits vers des Etats tiers, dans la mesure où ceux-ci ne jouissent pas d'un niveau de protection des données jugé adéquat. La directive a

également pour but de préciser et d'amplifier les principes contenus dans la Convention 108 (Convention du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel).

Bien que la Suisse ne soit pas membre de l'UE et n'appartienne pas à l'EEE, cette directive n'est pas sans intérêt, notamment dans le cadre des discussions bilatérales ou des développements législatifs en matière de protection des données. Elle devra également être prise en considération par les entreprises suisses déployant des activités au sein de l'UE impliquant le traitement de données personnelles. La LPD et la directive européenne ont une forte ressemblance, car elles ont été élaborées à la même période. Elles s'inspirent en outre toutes deux de la Convention 108. Des différences existent cependant: le régime des données sensibles, l'information des personnes concernées lors de la collecte ou de la communication des données, l'interdiction des décisions individuelles automatisées, l'étendue des droits d'accès et d'opposition de la personne concernée, la notification des traitements à l'autorité de contrôle, ainsi que les compétences et pouvoirs de cette autorité. Ces différences sont encore plus marquées à l'égard des cantons, notamment de ceux qui ne disposent pas de loi de protection des données et d'autorité de contrôle indépendante (voir aussi annexe p. 372 du présent rapport).

En ce qui concerne les flux transfrontières de données, la directive prévoit la libre circulation des données au sein de l'Union européenne. Vis-à-vis des pays tiers, la directive européenne prévoit que la communication de données personnelles à l'étranger n'est possible que si le pays destinataire assure un niveau de protection adéquat. En principe, les Etats ayant ratifié la Convention 108 du Conseil de l'Europe et disposant d'une autorité de contrôle indépendante devraient bénéficier d'un niveau de protection adéquat (voir à ce sujet, Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données»,http://www.europa.eu.int/comm/dg15/fr/index.htm).

Les organes compétents de la Commission de l'UE examinent actuellement la législation de plusieurs Etats tiers, dont la Suisse. Ils vont déterminer les Etats qui bénéficient d'un niveau de protection adéquat et préparer un ensemble de décisions à l'égard de ces Etats. Il s'agit d'une «déclaration d'adéquation positive». Dans ce cadre, le PFPD a été entendu par la commission. Cette dernière a été orientée sur la législation suisse, notamment sur les rapports entre le droit fédéral et le droit cantonal, y. c. pour le traitement de données personnelles en l'absence de dispositions cantonales de protection des données, sur le

régime des données sensibles, l'obligation d'information découlant du principe de la bonne foi et les registres publics.

Nous pouvons nous attendre à une déclaration d'adéquation positive de notre législation dans le courant de l'année 1999. Il n'en demeure pas moins nécessaire d'œuvrer afin de rendre eurocompatibles notre droit et notre pratique en matière de protection des données. Nous pouvons ainsi recommander aux entreprises établies en Suisse qui échangent ou traitent des données au sein de l'Union européenne de tenir compte des exigences de la directive. Cela concerne en particulier le devoir d'information des personnes concernées lors de la collecte ou de la communication des données. Celles-ci doivent être informées de l'identité du responsable du traitement, des finalités du traitement, des destinataires des données, du caractère facultatif ou obligatoire de la collecte et des conséquences d'un refus de réponse, ainsi que de l'existence des droits d'accès et de rectification. A propos de la communication de données à l'étranger, voir également le tableau annexé p. 371, 5ème rapport d'activités p. 221 et 3ème rapport d'activités p. 207.

3. Conférence internationale des commissaires

La XXe Conférence Internationale des Commissaires à la protection des données s'est déroulée à Saint-Jacques-de-Compostelle du 16 au 18 septembre 1998 à l'invitation de l'Agencia de Protección de Datos de l'Espagne. La Conférence réunissait les commissaires à la protection des données de 23 Etats du monde entier, des experts gouvernementaux, des représentants du Conseil de l'Europe et de la Commission européenne, ainsi que de l'industrie et de la science. Nous y avons présenté un exposé relatif à la «Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la coopération internationale à l'aube du XXIe siècle». Nous y plaidons en faveur d'un renforcement du droit international de la protection des données et de la coopération internationale, notamment en amendant la convention (reconnaissance d'un certain caractère d'application directe à la convention, introduction d'un droit individuel de recours, obligation de créer des instances de contrôle indépendantes, régime des flux transfrontières de données), en renforçant les compétences du comité consultatif de ladite convention, et en créant un comité des commissaires à la protection des Etats contractants.

La Conférence a abordé sept thèmes, à savoir:
l'utilisation des données publiques ou collectées à partir de sources accessibles au public, l'utilisation des nouvelles technologies pour le prélèvement de taxes routières, l'Internet, les flux transfrontières de données et le renforcement de la coopération internationale, les mesures de sécurité, le traitement des données à des fins de renseignements et de crédit, et la perception de l'individu pour la protection des données le concernant (autoprotection).
Chacun de ces thèmes a fait l'objet d'exposés de la part des commissaires ou de conférenciers invités.

En marge de la Conférence, les commissaires européens à la protection des données ont adopté deux résolutions. La première concerne la création d'une banque de données génétiques et médicales en Islande (http://www.cnil.fr/). L'Islande a en effet adopté une loi prévoyant la création d'un fichier central regroupant les dossiers médicaux de toute la population islandaise empreintes génétiques incluses. Ce fichier sera utilisé par une société pharmaceutique multinationale ayant son siège en Suisse. Il est destiné au contrôle de l'utilisation des services médicaux et des produits pharmaceutiques, et à la recherche. Dans leur résolution, les commissaires européens se montrent très préoccupés par ce projet et recommandent aux autorités islandaise de le reconsidérer à la lumière des principes fondamentaux consacrés dans la Convention européenne des droits de l'homme, la Convention 108 du Conseil de l'Europe et la Recommandation (97) 5 sur les données médicales, ainsi que par la directive européenne. Ils insistent sur le respect du principe du consentement préalable libre et informé de la personne concernée pour l'enregistrement des données la concernant, sur le recours à des méthodes garantissant un anonymat effectif et sur le strict respect du principe de finalité.

La seconde résolution (voir http://www.edsb.ch) concerne la protection des données personnelles et de la vie privée sur Internet. Elle fait suite à la publication sur Internet du rapport du Procureur Starr dans l'affaire Clinton/Lewinski. Dans cette déclaration, les commissaires européens, auxquels se sont associés les commissaires de l'Islande, de la Norvège et de la Suisse, soulignent le fait que certains usages d'Internet peuvent être contraires aux principes fondamentaux de la protection de la vie privée et de la protection des données personnelles. Ils rappellent la nécessité de reconnaître aux personnes concernées par l'usage de cette technologie des garanties en matière de protection des données personnelles et de la vie privée. Enfin, ils appellent à un renforcement de la coopération internationale dans ce domaine fondée sur la reconnaissance de principes universels.

4. OCDE

- Conférence ministérielle de l'OCDE à Ottawa sur le commerce électronique

Du 7 au 9 octobre 1998, une conférence de l'OCDE sur le commerce électronique s'est tenue à Ottawa (Canada). Outre les représentants des pays membres, un certain nombre d'organismes internationaux et de représentants de groupes d'intérêts, appartenant pour certains aux milieux touchant la protection des consommateurs et des données, étaient également présents. Il a été établi à l'issue de cette rencontre que la confiance des consommateurs est un aspect essentiel du développement du commerce électronique. La conférence a adopté entre autres une déclaration sur la protection de la sphère privée ainsi que des plans d'actions pour les futures activités de l'OCDE dans divers domaines.

Les conférences de l'OCDE sont avant tout un forum de discussion consacré à l'économie. Le commerce électronique a donc été envisagé surtout du point de vue économique. Un certain nombre de thèmes ont été traités de plus près à cette occasion: la libéralisation, le potentiel du marché et les perspectives d'avenir. L'appréhension des représentants de l'économie – qui craignent que les interventions de l'Etat dans le sens d'une régulation ne nuisent au potentiel de développement du commerce électronique – a été au centre de presque toutes les discussions. Par contre, le fait que l'Etat soit tenu de remplir ses obligations visant la garantie des intérêts publics n'a pas été véritablement abordé.
Certes, au cours des diverses interventions, la confiance des consommateurs et des utilisateurs à l'égard du commerce électronique a été sans cesse mise en valeur. Mais l'importance de la sphère privée, indispensable à l'élaboration de cette relation de confiance, n'a pas été suffisamment thématisée.

De ce fait, les déclarations adoptées par les ministres tant sur la signature digitale que sur la protection des consommateurs et des données manquent de fond. Les déclarations concernant la protection de la sphère privée sont trop générales car sans obligations précises pour l'économie privée. Cette formulation générale ne permettra pas de nourrir la confiance des consommateurs à l'égard du commerce électronique.

Un certain nombre de pays essentiellement européens, dont la Suisse, sont conscients de l'importance et de l'énorme potentiel du commerce électronique. Outre la création des conditions nécessaires à son épanouissement, ces pays entendent également tenir compte des intérêts de la protection des consommateurs et des données. La Suisse et la plupart des pays européens disposent de bases légales techniquement neutres et suffisamment larges pour assurer la

protection de la sphère privée. Ce cadre juridique n'empêche pas la recherche, nécessairement rapide dans notre société de communication, de solutions techniques adéquates et réalisables. Il pose en même temps des limites à la protection de la sphère privée dans le contexte du commerce électronique.

Le commerce électronique a besoin de solutions flexibles et variables. Les modèles d'autorégulation doivent donc associer harmonieusement intervention de l'Etat (conditions-cadres juridiques) et autorégulation du marché. Le cadre de cette autorégulation doit donc être mis en place en étroite coopération avec les autorités gouvernementales.

A l'occasion de la 5e réunion du Groupe d'experts sur la sécurité de l'information et la protection de la sphère privée des 21 et 22 octobre 1998, nous avons souligné la nécessité d'accompagner le développement du commerce électronique de travaux et de mesures assurant une protection effective de la sphère privée. Nous avons notamment souligné les points suivants:

- il convient d'appliquer les principes contenus dans les directives de l'OCDE sur la protection de la sphère privée.
- Les mesures préconisant l'autorégulation en matière de protection des consommateurs et des données doivent être claires et non équivoques sur les traitements qu'il est envisagé de faire subir aux données personnelles. Le consommateur doit pouvoir choisir librement entre l'un ou l'autre traitement. Il incombe en outre au prestataire de services de préciser le cadre juridique auquel il se soumet. Enfin, la validité juridique des mesures d'autorégulation dépend des possibilités offertes en matière de responsabilité.
- La validité des mesures d'autorégulation doit s'accompagner d'un cadre juridique.
- La protection de la sphère privée doit être appuyée par des méthodes techniques favorables à la protection des données (PET **p**rivacy **e**naching **t**echnologies).
- Les travaux de l'OCDE ne doivent pas se limiter à des échanges d'informations. Le développement du commerce électronique doit faire l'objet d'une surveillance régulière (monitoring) et il convient aussi de relever les progrès ou les carences.
- Enfin, l'OCDE doit chercher des méthodes efficaces permettant la protection de la sphère privée dans le cadre des différents modèles juridiques.

(voir également p. 359, Document présenté par la Suisse dans le contexte du commerce électronique et de la protection des données).

Il convient pour conclure de mentionner qu'au cours de la conférence, des associations de consommateurs ont posé des exigences similaires en vue d'assurer la protection de la sphère privée des utilisateurs. Pour ces organismes, la

protection des utilisateurs est un aspect essentiel du développement du commerce électronique.

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

Les travaux du Groupe de travail sur la sécurité de l'information et la protection de la sphère privée ont été essentiellement concentrés sur les préparatifs de la conférence d'Ottawa, en particulier sur les déclarations soumises à la décision des ministres participant à la conférence. La protection de la sphère privée a été un sujet de désaccord entre les Etats-Unis d'une part et les Etats européens et le Canada d'autre part.

Quelques Etats européens (dont la Suisse) ainsi que le Canada ne voulaient pas de déclarations à caractère uniquement déclaratif. Ils désiraient que ces déclarations obligent les gouvernements à assurer une protection effective de la sphère privée. C'était sans compter avec l'opposition des Etats-Unis et de quelques autres pays européens. De ce fait, la conférence s'est soldée par des déclarations au contenu très général du point de vue de la protection des données. Le désaccord entre les Etats membres de l'UE en matière de protection des données a servi les intérêts des Etats-Unis (à savoir protéger aussi peu que possible la sphère privée). Manifestement, les pays de l'UE n'ont su coordonner leur action de sorte que le représentant de la Commission européenne a dû, durant les négociations, défendre plusieurs fois seul les principes de la directive de l'UE sur le sujet.

Il est regrettable que le manque de coordination d'Etats dont les dispositions en matière de protection des données sont similaires, si ce n'est identiques, ait permis aux Etats-Unis de l'emporter. Ces Etats (membres du Conseil de l'Europe, Canada, Australie), n'auront à l'avenir d'autre choix que la coordination de leur action s'ils entendent contrer la politique extrêmement libérale des Etats-Unis (voir également à titre de comparaison les modèles d'autorégulation et la protection de la sphère privée, p. 317).

Au terme de la conférence d'Ottawa, le Groupe de travail sur la sécurité de l'information et la protection de la sphère privée a fait le bilan de la conférence et soumis aux différentes délégations le programme des travaux. Son objectif premier est de mettre sur pied des solutions pratiques et techniques pour garantir la protection de la sphère privée dans le monde virtuel. Nous avons à cette occasion présenté un document de principe sur les exigences minimales que requiert la protection de la sphère privée dans le contexte du commerce électronique (voir p. 359 en annexe).

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

Le PFPD a participé à la 24e réunion du groupe de travail les 9 et 10 novembre 1998 à Berlin. Le groupe élabore et publie des prises de position communes ainsi que des mémorandums dans le domaine des télécommunications et des médias et promeut la discussion et l'échange d'informations parmi les représentants des préposés à la protection des données. Les thèmes principaux de la séance d'automne 1998 étaient: l'évolution du droit des télécommunications dans un contexte récemment libéralisé (dans nombre de pays), les réglementations gouvernementales de l'utilisation de procédés cryptographiques ainsi que des questions relatives à la protection des données dans l'Internet, en particulier la publication de données publiquement accessibles (voir aussi: http://www.datenschutz-berlin.de/doc/int/index.htm#iwgdpt).

IV. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

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

La cinquième Conférence suisse des Commissaires à la protection des données s'est déroulée à l'université de Fribourg, le 13 octobre 1998. Elle était organisée par l'autorité fribourgeoise de protection des données. Cette conférence a réuni le Préposé fédéral à la protection des données, les Commissaires cantonaux et communaux de la protection des données, ainsi que les conseillers à la protection des données de l'administration cantonale de Fribourg. Elle a été suivie d'un colloque consacré au droit européen de la protection des données organisé par l'Institut de droit européen de l'Université de Fribourg.

Les sujets suivants ont été abordés: la suite donnée à la résolution de la 4e conférence concernant les codes CIM-10 (voir 5e rapport d'activités 1997/98, p. 247 et 269), le recensement de la population en l'an 2000, les résultats de l'enquête du PFPD dans le domaine de téléphonie mobile, le registre ADN dans les procédures pénales, la protection des données au-delà de la mort, le traitement de données personnelles à des fins de police (notamment videosurveillance sur les autoroutes et outsourcing des données de police), la protection des données et les téléphones sur le lieu de travail, ainsi que le droit de blocage lors

de la communication des données personnelles par les organes cantonaux ou communaux.

En ce qui concerne le registre ADN, la conférence a, à l'unanimité, adopté une résolution (voir www.edsb.ch). Depuis quelque temps, les autorités de poursuite pénale recourent à des analyses génétiques ADN pour élucider des actes criminels. Les empreintes génétiques permettent ainsi d'identifier un coupable ou de disculper un innocent. Elles fournissent également d'autres informations, notamment sur la parenté. Si le matériel cellulaire est conservé, il peut d'autre part révéler des informations sur les prédispositions à des maladies et le patrimoine héréditaire des personnes concernées. Ces analyses ADN comportent des risques pour les droits fondamentaux des individus. La conservation d'échantillons et des résultats de leur analyse ADN une fois la personne concernée innocentée ou la procédure pénale close constitue une atteinte au principe de présomption d'innocence (ATF 124 I 80).
La conférence suisse des commissaires à la protection des données exige l'adoption des bases légales nécessaires préalablement à la mise en place d'un registre ADN à des fins de poursuites pénales et à la conservation du matériel génétique. La conservation des échantillons d'identification devrait être limitée dans le temps. Le matériel cellulaire ne devrait en principe pas être conservé après la clôture de la procédure pénale, du prononcé d'un non lieu ou de la suspension de la procédure (voir p. 285).

En ce qui concerne le droit de blocage, la conférence a constaté que les registres publics et notamment ceux des contrôles de l'habitant sont sollicités dans les buts les plus divers. Afin de permettre au citoyen de garder la maîtrise sur les données le concernant, la Conférence suisse des Commissaires à la protection des données rappelle l'existence d'un droit de s'opposer à la communication de ses données personnelles notamment à des fins publicitaires et commerciales. Elle recommande l'introduction dans la législation – si cela n'est pas encore prévu - d'un droit général (sans obligation de motivation) de s'opposer à la communication de ses données personnelles à des fins publicitaires et commerciales. Elle invite enfin les autorités cantonales et communales à informer leurs citoyens de ce droit (voir p. 301).

Pour sa part, le groupe de travail des préposés cantonaux à la protection des données, avec lequel le PFPD collabore étroitement, a abordé en particulier des questions dans le domaine de la santé et de la génétique, de la statistique (notamment le recensement de la population), de l'emploi (surveillance téléphonique sur le lieu de travail qui fera l'objet d'une directive), de la police, de la sécurité des données et du commerce d'adresses.

2. Le concept de formation du PFPD

En plus des cours usuels concernant la protection des données, le PFPD a élaboré un concept de formation. Il s'adresse surtout aux directeurs, aux conseillers à la protection des données et aux responsables informatiques. Le concept prévoit l'établissement de contacts entre ces groupes de personnes. Quant à la formation, elle sera adaptée spécifiquement aux besoins des personnes cibles. Le projet démarrera en 1999 dans l'administration fédérale. Il est cependant prévu d'étendre également le concept au secteur privé.

Le concept de formation doit permettre d'atteindre plusieurs objectifs. Ainsi, on y présente entre autres les exigences principales de la protection des données, les risques possibles, les avantages personnels qui en résultent pour les groupes cibles ainsi que les responsabilités.
Il doit permettre de réunir les personnes qui jouent un rôle clé pour le respect des dispositions de protection des données tels que directeurs, conseillers à la protection des données et responsables informatiques. A l'aide d'un plan d'action, les conseillers à la protection des données et les responsables informatiques démontrent à leur directeur les risques qui existent et proposent des mesures permettant de les éliminer. Lors d'une séance périodique, le directeur attribue des priorités à ces mesures et charge un responsable de les appliquer. Il s'informe également sur l'état d'avancement de mandats antérieurs. Ces séances servent également au conseiller à la protection des données de base pour procéder aux nouvelles annonces et aux mises à jour dans le registre des fichiers auprès du PFPD. Dans la mesure ou des contrôles internes ont été prévus, il importe également que l'on oriente, lors de ces séances, les personnes impliquées sur les résultats obtenus. Finalement, ces séances montrent quelle importance la direction attache à la protection et à la sécurité des données.
La principale question qui se pose lors de la formation de responsables informatiques et d'équipes de projet est comment rendre les systèmes d'information conformes aux exigences de la protection des données. Il s'agit en l'occurrence de créer une transparence totale en ce qui concerne les rôles, les buts, les activités ainsi que les données nécessaires à ces fins. Ceci permet alors d'évaluer si le traitement de données est proportionnel.
Les séances de formation ont notamment pour but d'écarter les malentendus, de découvrir des synergies et de promouvoir une bonne collaboration.

3. Les publications du PFPD (Nouvelles parutions)

- Feuille d'information 1/98
- Feuille d'information 1/99

Nous avons une nouvelle publication, la «feuille d'information du PFPD». A travers elle, nous voulons en particulier informer les personnes concernées de leurs droits et ainsi les aider à protéger leur vie privée.

4. Statistique des activités du PFPD
Période du 1er avril 1998 au 31 mars 1999

5. 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
Suppléante :	Grand Carmen, lic. en droit
Délégué Presse et Information :	Tsiraktsopulos Kosmas, lic. en droit
Service juridique :	Atia-Off Katrin, dr en droit Buntschu Marc, lic. en droit Costa Giordano, lic. en droit Horschik Matthias, Fürsprecher Kardosch Milica, lic. en droit Schnyder Michael, lic. en droit, informaticien Schönbett Frédéric, lic. en droit Tsiraktsopulos Kosmas, lic. en droit Wiederkehr Rita, Fürsprecherin
Service informatique :	Scherrer Urs, informaticien Schnyder Michael, lic. droit, informaticien Stüssi Philipp, lic. sc. nat., informaticien
Chancellerie :	Blattmann Doris Purro Isabelle Rappo Nicole

V. ANNEXES

1. Commerce électronique et protection de la sphère privée

Document remis par le PFPD dans le cadre des travaux du groupe de travail de l'OCDE

Il convient d'accorder une place centrale aux intérêts et vœux des consommateurs dans les décisions politiques sur les transactions commerciales. En effet, le développement des échanges commerciaux électroniques ne peut s'envisager sans les consommateurs. Pour cette raison, il est nécessaire de prendre des mesures permettant de renforcer la confiance des consommateurs envers les échanges commerciaux électroniques, notamment par les mesures suivantes de protection de la sphère privée:

- dans la mesure du possible, la collecte de données personnelles sera limitée aux données nécessaires à une transaction déterminée. Parallèlement, il convient de promouvoir les transactions anonymes.
- Les utilisateurs doivent pouvoir contrôler la collecte, l'utilisation et la communication de leurs données personnelles.
- S'il y a violation de sa sphère privée, l'utilisateur doit avoir les moyens juridiques de faire valoir ses droits.
- Le commerce électronique doit offrir la même protection juridique que les relations commerciales traditionnelles. Cette protection juridique peut être garantie par la révision de lois et si nécessaire aussi par des règles de comportement. Enfin, il faut fournir aux utilisateurs les moyens nécessaires pour que les transactions en ligne ne portent pas atteinte à leur sphère privée.

Diverses recherches récemment effectuées ont montré que la sphère privée des consommateurs et des utilisateurs n'est pas protégée lorsqu'il y a transactions en ligne (notamment Internet). Pour cette raison, les autorités doivent veiller à ce que non seulement les représentants de l'économie, mais aussi les organismes indépendants de protection des données et associations de consommateurs soient associés à la mise au point de règles de comportement. Il convient en outre de limiter la collecte de données personnelles aux données nécessaires à une transaction déterminée.

Le secteur privé est appelé à jouer un rôle déterminant dans l'expansion des échanges commerciaux électroniques. Les autorités pour leur part auront pour tâche de suivre avec attention cette évolution et devront prendre les mesures nécessaires dans les domaines où les dispositions d'autorégulation telles les règles de comportement ne peuvent garantir avec efficacité la confiance dans les échanges électroniques et la protection de la sphère privée.

L'intervention des autorités ne signifie pas qu'il faille en tout cas établir des règles juridiques. La sphère privée peut aussi être protégée au moyen de mesures d'autorégulation. Celles-ci ne doivent néanmoins pas être seulement théoriques, mais aussi effectives.

2. Lignes directrices du Conseil de l'Europe sur la protection de la vie privée sur Internet

Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les "inforoutes", qui peuvent être intégrées ou annexées à des codes de conduite

I. Introduction

Les présentes lignes directrices énoncent des principes d'une conduite loyale à observer en matière de protection de la vie privée par les utilisateurs et les fournisseurs de services d'Internet [note 1]. Ces principes peuvent être repris dans des codes de conduite.

Les utilisateurs devraient être conscients des responsabilités des fournisseurs de services d'Internet et vice versa. Il est donc conseillé aux utilisateurs et aux fournisseurs de services d'Internet de lire ce texte en entier, bien qu'il soit divisé en plusieurs parties pour le rendre plus facile à utiliser. Vous pouvez être concerné par une seule ou plusieurs parties de ce texte à la fois.

L'utilisation d'Internet implique une responsabilité pour chaque action et comporte des risques pour la vie privée. Il est important de se conduire de manière à se protéger et à promouvoir de bonnes relations avec les autres. Ces lignes directrices énoncent quelques solutions pratiques pour la protection de la vie privée, mais ne vous dispensent pas de connaître vos droits et obligations.

Rappelez-vous que le respect de la vie privée est un droit fondamental de tout individu qui peut être protégé également par des lois sur la protection des données. Alors, mieux vaut vérifier votre situation juridique.

II. Pour les utilisateurs

1. Rappelez-vous qu'Internet n'est pas sûr. Cependant, existent et se développent différents moyens vous permettant d'améliorer la protection de vos données [note 2]. Utilisez donc tout moyen disponible pour protéger vos données et vos communications, tel que le cryptage légalement disponible pour des courriers électroniques confidentiels aussi bien que des codes d'accès à votre propre PC [note 3].

2. Rappelez-vous que chaque transaction effectuée, chaque visite d'un site sur Internet laissent des traces. Ces "traces électroniques" peuvent être utilisées à votre insu pour établir un profil de votre personne et de vos intérêts. Si vous ne voulez pas que votre profil soit établi, vous êtes encouragé à utiliser les dispositifs techniques les plus récents qui comprennent la possibilité d'être informé à chaque fois que vous laissez des traces et à refuser ces traces. Vous pouvez également demander à être informé des règles de conduite retenues par les différents programmes et sites en matière de protection de la vie privée et préférer ceux qui enregistrent peu de données ou qui sont accessibles d'une manière anonyme.

3. L'accès et l'utilisation anonymes des services et des paiements constituent la meilleure protection de la vie privée. Informez-vous des moyens techniques de recourir à cet anonymat, si cela est approprié [note 4].

4. L'anonymat absolu peut ne pas être approprié en raison de contraintes légales. Dans ce cas, si la loi l'autorise, vous pouvez utiliser un pseudonyme, de sorte que votre identité véritable ne sera connue que de votre fournisseur de services d'Internet.

5. Ne communiquez à votre fournisseur de services d'Internet ou à toute autre personne que les données qui sont nécessaires pour une finalité déterminée dont vous avez été informé. Soyez particulièrement vigilant avec les cartes de crédit et les numéros de compte, qui peuvent être très facilement utilisés - abusivement - dans le cadre d'Internet.

6. Rappelez-vous que votre adresse électronique constitue une donnée à caractère personnel et que d'autres peuvent souhaiter l'utiliser à différentes fins, telles que son inclusion dans des annuaires ou des listes d'utilisateurs. N'hésitez pas à demander quelle est la finalité de ces annuaires ou de ces autres utilisations. Vous pouvez demander que votre adresse soit effacée si vous ne souhaitez pas figurer dans ces annuaires ou dans ces listes.

7. Soyez prudent à l'égard des sites qui demandent plus de données que nécessaire pour l'accès au site ou la réalisation d'une transaction, ou encore qui ne vous précisent pas pourquoi ils ont besoin de l'ensemble de ces données vous concernant.

8. Rappelez-vous que votre responsabilité juridique est engagée pour le traitement de données, par exemple si vous téléchargez ou télédéchargez illicitement et que, même si vous avez utilisé un pseudonyme, on peut vous identifier.

9. N'envoyez pas de courrier malveillant, cela peut se retourner contre vous et avoir des conséquences juridiques.

10. Votre fournisseur de services d'Internet est responsable de la bonne utilisation des données. Demandez-lui quelles données il collecte, traite et conserve, de quelle manière, et pour quelles finalités. Répétez cette demande de temps en temps. Exigez qu'il les modifie si elles sont inexactes ou qu'il les efface si elles sont excessives, si elles ne sont pas mises à jour ou ne sont plus nécessaires. Demandez au fournisseur de services d'Internet qu'il notifie cette modification aux autres parties auxquelles il a communiqué vos données [note 5].

11. Si vous n'êtes pas satisfait de la manière dont votre fournisseur de services d'Internet actuel collecte, traite, conserve ou communique vos données et s'il refuse de modifier son attitude, alors envisagez de changer de fournisseur. Si vous estimez que votre fournisseur de services d'Internet ne respecte pas les règles relatives à la protection des données, vous pouvez informer les autorités compétentes ou intenter une action en justice.
12. Informez-vous des risques pour la vie privée et la sécurité sur Internet ainsi que des moyens disponibles de réduire ces risques.
13. Si vous avez l'intention d'envoyer des données vers un autre pays, vous devez être conscient du fait que ces données peuvent y être moins bien protégées. S'il s'agit de vos propres données, vous êtes évidemment libre de les transmettre malgré tout. Cependant, avant d'envoyer vers un autre pays des données concernant d'autres personnes, informez-vous, par exemple auprès de vos autorités, sur la possibilité de procéder à ce transfert note 6. Le cas échéant, vous devrez demander à la personne qui reçoit les données de prendre les garanties note 7 nécessaires pour assurer la protection des données.

III. Pour les fournisseurs de services d'Internet

1. Utilisez les procédures appropriées et les technologies disponibles, de préférence celles faisant l'objet d'une certification, garantissant la vie privée des personnes concernées (même si elles ne sont pas utilisatrices d'Internet) et notamment l'intégrité et la confidentialité des données ainsi que la sécurité physique et logique du réseau et des services fournis sur le réseau.
2. Informez les utilisateurs des risques que l'utilisation d'Internet fait courir à la vie privée, avant qu'ils ne souscrivent ou commencent à utiliser des services. Il peut s'agir de risques concernant l'intégrité des données, leur confidentialité, la sécurité du réseau ou d'autres risques liés à la vie privée, tels que la collecte ou l'enregistrement de données effectués à leur insu.
3. Informez l'utilisateur des moyens techniques qu'il peut utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications, tels que le cryptage et les signatures électroniques légalement disponibles. Proposez ces moyens techniques à un prix orienté par les coûts et non dissuasif.
4. Avant d'accepter des abonnements et de connecter des utilisateurs à Internet, informez ces derniers des moyens d'y accéder, d'utiliser ses services et de les payer anonymement (par cartes d'accès prépayées par exemple). L'anonymat absolu peut ne pas être approprié en raison de contraintes légales. Dans ce cas, si la loi l'autorise, offrez la possibilité d'utiliser des pseudonymes. Informez les utilisateurs de l'existence de programmes permettant d'effectuer des recherches et de naviguer anonymement sur Internet. Concevez votre système d'une manière qui évite ou réduise au minimum l'utilisation de données.
5. Ne lisez pas, ne modifiez pas et ne supprimez pas les messages envoyés à d'autres.
6. Ne permettez aucune ingérence dans le contenu des communications, sauf si cette ingérence est prévue par la loi et est effectuée par une autorité publique.
7. Ne collectez, traitez et conservez des données sur les utilisateurs que lorsque cela est nécessaire pour des finalités explicites, déterminées et légitimes.
8. Ne communiquez pas de données à des tiers, sauf si la communication est prévue par la loi note 8.
9. Ne conservez pas de données pour une période plus longue que ce qui est nécessaire pour atteindre le but du traitement note 9.
10. N'utilisez des données aux fins de promouvoir ou de commercialiser vos propres services que si la personne, après avoir été informée, n'y a pas mis d'objection ou si, en cas de traitement de données de trafic ou de données sensibles, elle y a consenti explicitement.
11. Vous êtes responsable de la bonne utilisation des données. Sur votre page de bienvenue, affirmez par une indication claire et visible votre politique en matière de vie privée. Cette indication devrait permettre, par un « hyperlien », d'accéder à une explication détaillée de vos pratiques en matière de vie privée. Avant que l'utilisateur ne commence à utiliser des services, lorsqu'il visite votre site et chaque fois qu'il en fait la demande, informez-le de votre identité, des données que vous collectez, traitez et conservez, de quelle manière, pour quelles finalités et pour quelle durée vous les conservez. Au besoin, demandez-lui son consentement. A la demande de la personne concernée, rectifiez sans attendre les données inexactes, effacez-les si elles sont excessives, si elles ne sont pas mises à jour ou si elles ne sont plus nécessaires, et arrêtez le traitement des données si l'utilisateur s'y oppose. Notifiez aux tiers auxquels vous avez communiqué les données toute modification. Evitez toute collecte de données effectuée à l'insu de l'intéressé.
12. L'information fournie à l'utilisateur doit être exacte et mise à jour.
13. Réfléchissez à deux fois avant de publier des données sur votre site ! Une telle publication pourrait porter atteinte à la vie privée d'autres personnes et pourrait aussi être interdite par la loi.
14. Avant d'envoyer des données à destination d'un autre pays, informez-vous, par exemple auprès de vos autorités, sur la possibilité de procéder à ce transfert note 10. Le cas échéant, vous devrez demander à la personne qui reçoit les données de prendre les garanties note 11 nécessaires pour assurer la protection des données.

IV. Clarifications et recours

1. Lorsque, dans ce texte, les termes "fournisseur" ou "prestataire de service" sont utilisés, ils s'appliquent également, le cas échéant, aux autres acteurs d'Internet tels que les fournisseurs d'accès, de contenu, de réseau, les concepteurs de logiciels de navigation, les coordinateurs de forums ou d'« info-kiosques », etc.

2. Il est important de vous assurer du respect de vos droits. Les mécanismes de feedback offerts par des forums d'Internet, les associations de fournisseurs de services d'Internet, les autorités de protection des données ou autres instances sont des moyens importants pour assurer le respect de ces lignes directrices. Contactez-les si vous avez besoin de clarifications ou de recours.

3. Ces lignes directrices s'appliquent à tout type d'"inforoute".

---

1 Voir partie IV, paragraphe 1.

2 Le terme "donnée" se rapporte aux données à caractère personnel et signifie toute information vous concernant ou concernant d'autres personnes.

3 Par exemple, utilisez des mots de passe et modifiez-les régulièrement.

4 Par exemple en utilisant des kiosques Internet publics ou des cartes d'accès prépayées et des cartes de paiement.

5 Les lois de protection des données, à l'instar de l'article 5 de la Convention sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, du Conseil de l'Europe, rendent celui qui les traite responsable de l'exactitude et de la mise à jour des données.

6 La législation de nombreux pays en Europe interdit les transferts vers les pays n'ayant pas un niveau de protection des données adéquat ou équivalent à celui de votre pays. Des exceptions sont toutefois prévues, notamment si la personne concernée a consenti à ce que ses données soient transmises vers de tels pays.

7 Ces garanties peuvent être développées et/ou présentées, notamment dans le contrat régissant le flux transfrontière de données.

8 Généralement, les lois en matière de protection des données permettent sous diverses conditions la communication à des tiers, notamment:

- de données sensibles et de données de trafic, à condition que la personne concernée y ait explicitement consenti;

- d'autres données lorsque la communication est nécessaire pour atteindre la finalité légitime poursuivie ou lorsque la personne concernée, après avoir été informée, ne s'y est pas opposée.

9 Par exemple, ne conservez pas des données de facturation, à moins que cela ne soit prévu par la loi.

10 Voir note 6.

11 Voir note 7.

3. Déclaration des autorités indépendantes de protection des données.
XXe Conférence internationale de Saint Jacques de Compostelle (Espagne), 15-17 septembre 1998

DECLARATION

Les autorités indépendantes de protection des données et de la vie privée des États de l'Union européenne, en association avec les autorités indépendantes de protection des données et de la vie privée d'Islande, de Norvège et de Suisse, à l'issue de la vingtième conférence annuelle internationale des autorités indépendantes de protection des données et de la vie privée qui s'est tenue à Saint Jacques de Compostelle (Espagne), les 15-17 septembre 1998 :

CONVAINCUES qu'Internet constitue un moyen d'approfondissement de la démocratie, notamment en permettant une plus large participation des citoyens aux débats publics et en assurant une plus grande transparence des activités publiques ;

APPELLENT L'ATTENTION sur le fait que :
- l'usage d'un tel moyen de diffusion et de collecte de l'information et ses éventuelles conséquences à l'égard de principes fondamentaux nécessitent la reconnaissance de garanties ;
- ces garanties, qui ne doivent pas faire obstacle à la liberté d'expression ni au droit à l'information, doivent être établies au plan mondial ;

ESTIMENT que sur la base des principes déjà établis dans de nombreux pays en matière de protection des données personnelles et qui sont applicables à Internet, l'ensemble des États, et tout particulièrement ceux qui recourent le plus aux nouvelles technologies, doivent adopter et mettre en œuvre des mesures de protection des données personnelles et promouvoir une coopération internationale fondée sur la reconnaissance de principes universels pour empêcher que l'utilisation croissante d'Internet produise des effets incompatibles avec la protection des données personnelles et de la vie privée,

et **NOTAMMENT** :
- que les données susceptibles d'être détournées pour porter atteinte ou harceler les personnes ne soient pas diffusées sur Internet dans des conditions permettant de tels détournements ;
- que des moyens légaux et techniques efficients soient développés afin de permettre aux personnes de déterminer elles même et de contrôler l'usage de leurs données ;
- que des moyens soient mis en œuvre pour assurer une application effective des principes de la protection des données par l'ensemble des acteurs qui diffusent ou collectent des données personnelles sur Internet ou qui assurent l'infrastructure du réseau.

4. Recommandations pour une présentation des sites Web conforme à la protection des données (Expertise de l'OCDE)

SUGGESTIONS POUR UN DESIGN *PRIVACY FRIENDLY* DES SITES *WEB*

1. Cookies

- Le visiteur d'un site Web doit être informé de la finalité de la collecte et des traitements de données relatifs aux *cookies* au moment où ceux-ci sont placés dans le fichier correspondant de son *browser*.

- La durée de conservation des *cookies* et plus largement de toute information personnelle doit être définie et non excessive ; une durée de vie d'un ou deux ans semblerait acceptable ; des durées plus longues peuvent être admises en fonction de la durée du contrat liant un utilisateur et un service en ligne sur lequel il se connecte régulièrement : dans ce cas la durée de conservation doit être proportionnelle à la durée pendant laquelle la prestation est fournie, plus une période d'environ un an pour régler les contestations éventuelles liées à la facturation ou à des fins de reconquête du client.

- L'implantation de *cookies* en rafale provoquant un effet de saturation chez le visiteur devrait être résolument déconseillée.

- Lorsqu'un utilisateur a formulé une première fois son refus d'acceptation d'un *cookie*, le site Web devrait cesser définitivement ses tentatives d'implantation.

- Aucun lien de subordination ne devrait exister entre le fait d'accepter un *cookie* ou plus largement de transmettre des informations personnelles et la possibilité de naviguer librement à travers les pages et les rubriques publiques d'un site Web.

- L'information sur les finalités des *cookies* doit être sincère et complète : elle doit permettre notamment de distinguer les finalités et les traitements de données selon que les *cookies* sont implantés par les sites eux-mêmes ou par des agences de publicité.

- L'information doit également comporter des indications précises sur l'existence de *matchings* entre les données d'identification (voir suggestion numéro8) et les données navigationnelles issues des *cookies*.

2. Messages électroniques (E-mail)

- Toute transmission de message de demande d'informations à un site dévoile indirectement l'adresse *e-mail* de l'émetteur ; dans le cadre d'une obligation de conseil, il est de la responsabilité des sites d'en avertir leurs visiteurs.

3. Formulaires

- Les informations facultatives collectées à travers les différents formulaires (inscriptions, enquêtes, feed-back, paiement) doivent être clairement séparées des informations obligatoires et regroupées dans un bloc distinct.

- Si des données sensibles sont collectées de manière légitime, le site doit s'engager à respecter à leur égard le plus haut niveau de sécurité et de confidentialité.

4. Cession de données à des tiers et opposition (opt-out)

- Tout site qui collecte des données personnelles doit offrir à ses visiteurs une possibilité d'*opt-out* en ligne.

- Les possibilités d'*opt-out* doivent pouvoir s'exercer directement et simultanément à lacollecte au moyen d'un cochage de case sur les formulaires de collecte même.

- L'exercice de l'*opt-out*, dans les cas où cela s'impose, doit distinguer à quels traitements il s'applique : aux traitements commerciaux réalisés par le site lui-même, aux traitements d'analyse navigationnelle, aux extractions de listes destinées à des tiers et aux *matchings* dont ces listes pourraient faire l'objet par la suite.

- L'*opt-out* doit pouvoir s'exercer également en direction des agences de publicité qui réalisent des ciblages *one-to-one* ; à cette fin les sites Web doivent pouvoir soit s'engager à recueillir cet *opt-out* et à le transmettre à l'agence, soit fournir un hyper-lien qui permette de se connecter directement sur la bonne page du site publicitaire afin que l'utilisateur puisse lui-même exécuter la procédure.

- Tout site qui, après s'être engagé à ne fournir aucune donnée personnelle à des tiers, souhaite néanmoins le faire, doit obtenir le consentement préalable de la personne concernée. Une modification unilatérale des *Terms Of Service* n'est en aucun cas suffisante.

5. Education/Information

- Tout site Web se référant à l'application d'un instrument international ou régional de protection des données est encouragé à faire expressément référence à cet instrument et à fournir un hyper-lien avec le site de l'organisation concernée.

- Tout site Web opérant à partir d'un pays qui dispose d'une loi nationale en matière de protection des données doit y faire référence formellement et dans le cadre de la politique générale d'information et d'éducation des utilisateurs, fournir un hyper-lien avec le site de l'autorité administrative responsable de la bonne application de ladite loi. Il y a à cet égard une nécessité pressante que chaque autorité de protection des données existant dans le monde soit présente sur le Web à travers des sites pertinents, documentés et interactifs.

- Tout site Web se réclamant d'un instrument professionnel ou sectoriel doit fournir un hyper-lien avec le texte du code auquel il est fait référence et avec le site de l'organisation professionnelle responsable de sa bonne application.

6. Transparence des sites

- Quel que soit l'instrument international ou national dont ils se réclament, les sites doivent, parce qu'ils opèrent à l'échelle mondiale, se doter de "*privacy statements*" accessibles en ligne par leurs visiteurs.

- Les "*privacy statements*" accessibles en ligne doivent au minimum être explicites quant aux données collectées, quant à leur justification, quant à l'utilisation des *clickstream data* et des traitements dont elles font l'objet et quant aux possibilités d' *opt-out*.

- La mention faisant référence aux *"privacy statements"* doit figurer explicitement et de manière visible sur le *homepage* de chaque site concerné.

- Tout site implanté dans un pays où la loi nationale exige une déclaration préalable des traitements doit mentionner le numéro de récépissé délivré par l'autorité compétente.

- Tout site se réclamant de l'application d'un code de bonne conduite sectoriel doit le mettre en œuvre scrupuleusement dans la totalité de ses dispositions.

7. Sécurité

- Les sites commerciaux qui offrent des procédures de paiements *on line* doivent obligatoirement mettre à niveau leur plate-forme serveur de manière à intégrer aussitôt qu'ils sont disponibles et éprouvés les moyens les plus sécurisés.

- Les sites commerciaux qui offrent à la vente des produits ou des services achetables pour de petits montants doivent accepter les moyens de paiement anonymes.

- Dans le cadre de leur obligation de conseil à leurs visiteurs, les sites qui traitent des données confidentielles doivent alerter leurs visiteurs quant aux risques de divulgation de leurs données qui existent localement sur leur micro-ordinateur (historique des consultations, fichier cache).

- En l'absence pour l'instant de sécurité absolue en matière d'authentification des paiements et de transmission de données sur le réseau, les sites commerciaux qui acceptent les paiements *on line* à l'aide de cartes bancaires peuvent configurer leur système de telle sorte à ne réclamer qu'une seule fois les coordonnées de la carte à la condition impérative de stocker cette information dans des fichiers hautement sécurisés, sur des ordinateurs non-connectés au réseau *(non-networked computers)*.

8. Droits individuels

- Tous les sites pratiquant le commerce électronique doivent offrir à leurs clients des procédures de recours par *e-mail.*

- Tous les sites collectant des données personnelles doivent fournir à leurs visiteurs identifiés la possibilité d'exercer leur droit d'accès *on line ;* à défaut ce droit doit pouvoir s'exercer *off line* et dans ce cas l'adresse postale du site doit figurer en bonne place.

- Le droit d'accès doit pouvoir s'exercer de manière complète et ne pas être limité aux seules données fournies par les visiteurs du site. Si des données sont collectées ou générées par ailleurs, si par exemple des profils de navigation ou d'achat sont constitués, les visiteurs exerçant leur droit d'accès doivent également avoir communication de cette information et notamment du segment comportemental dans lequel ils sont classés.

- Au cas où l'information demandée à travers l'exercice du droit d'accès ne serait matériellement pas possible à transmettre, le site doit motiver sa réponse dans des formes précises et intelligibles à un non-initié.

9. Technologies protectrices de la vie privée (Privacy Enhancing Technologies)

- Les sites Web doivent s'engager à mettre en œuvre sur leur plate-forme serveur, aussitôt qu'elles seront disponibles et éprouvées, les solutions techniques de protection des données personnelles intégrées aux *browsers (PETs),* dès lors que ces solutions apportent une réponse aux suggestions ci-dessus et permettent aux utilisateurs de définir et rectifier au coup par coup la délivrance de leur données personnelles en fonction des différentes catégories de destinataires possibles.

10. Responsabilité

- Tous les sites Web collectant des données personnelles doivent formellement admettre le principe de leur responsabilité pleine et entière par rapport à la sécurité, à la confidentialité et à tous les engagements pris de façon déclarative ou contractuelle quant à ces données et à leurs traitements.

5. Feuille d'information sur les études de marché et sondages d'opinion à des fins privées

Le Préposé fédéral à la protection des données informe :

INFORMATION SUR LES ÉTUDES DE MARCHÉ ET SONDAGES D'OPINION À DES FINS PRIVEES

Les adresses et autres données personnelles de clients potentiels ont une influence décisive sur l'efficacité du marketing direct. En effet, des données aussi exactes que possible sur l'âge, la profession, le comportement de consommation etc. contribuent à réduire le risque de publicité inutile. Parmi la population, on constate une grande prédisposition à communiquer des données, même très personnelles, lorsque la personne interrogée croit participer à un projet scientifique. Un procédé particulièrement fructueux consiste à lier de tels sondages à la participation à un concours ou un jeu. Les clients potentiels sont ainsi amenés à remettre *de plein gré* des données les concernant. Ce genre de collecte commerciale camouflée (relevés pseudo-scientifiques) et les démarches publicitaires non reconnaissables en tant que telles ne sont pas autorisés.

Etudes de marché et sondages d'opinion effectués par écrit

Vous recevez, par courrier, un questionnaire sur un thème précis émanant d'un institut de sondage ou d'une société.
Sachez que vous n'êtes pas tenus de participer à ce sondage.
Si vous voulez tout de même y participer, vous devez savoir exactement à quoi vous vous engagez en répondant aux questions. En général, les personnes qui ont élaboré le questionnaire se contentent de décrire brièvement le but de l'enquête. Parfois aussi, le questionnaire est directement lié à un concours, à un tirage au sort ou autre cadeau. Ce procédé n'est toutefois pas correct et de ce fait illicite. Les personnes qui posent les questions doivent vous informer clairement et sans équivoque et ne pas éveiller en vous de fausses idées.

Vous devez veiller aux points suivants:
- Sur le mandat de quelle entreprise ou personne la collecte de données est-elle effectuée?
- Une communication de vos données personnelles à une entreprise tierce est-elle prévue? Si oui, à qui et à quelles fins?
- L'utilisation de vos données personnelles est-elle indiquée?
- La partie "réponses" proprement dite peut-elle être séparée de la possibilité de participer à un tirage au sort ou autre concours?

Si la réponse à l'une de ces questions est "non", il est douteux que le questionnaire soit correct et vous devriez y regarder à deux fois avant de participer. En effet, dans bien des cas, l'objectif du sondage n'est qu'un prétexte, le but véritable du questionnaire restant quand à lui dans le flou.

Par ailleurs, si vous recevez ce genre de questionnaire adressé directement à votre nom, vous pouvez bloquer votre adresse pour qu'elle ne soit plus utilisée à des fins publicitaires.

Si vous désirez d'autres informations, vous pouvez commander auprès du préposé la feuille d'information consacrée au blocage des adresses à des fins publicitaires.

Etudes de marché et sondages d'opinion effectués par téléphone

Le téléphone sonne. Vous décrochez et quelqu'un vous demande si vous êtes disposé à participer à un sondage d'opinion et à répondre à quelques questions.

Ce genre de sondage est susceptible d'empiéter sur votre liberté personnelle. Néanmoins, bien des personnes répondent au téléphone à des questions personnelles en donnant force détails et communiquent ainsi des informations qu'ils ne donneraient même pas à une connaissance.
Même des questions tout à fait anodines sur votre comportement de consommation, vos loisirs, etc. peuvent avoir des conséquences désagréables.
La participation souvent trop empressée des personnes sondées a souvent pour origine l'effet de surprise voulu de ce type d'enquête, ainsi que l'incapacité des personnes contactées à dire "non".

N'oubliez pas: vous n'êtes pas tenus de participer à ces enquêtes!

Ne vous laissez pas surprendre, et avant de révéler des informations sur votre propre personne, nous vous recommandons - si vous désirez participer - de requérir les informations suivantes:

- numéro de téléphone et adresse de l'entreprise qui fait effectuer la collecte de données
- nom de la personne qui appelle
- but de l'enquête
- utilisation de vos données.

Au cas où la personne qui appelle ne décline pas son identité, ou si les indications qu'elle fournit semblent douteuses, mettez fin à la conversation téléphonique.
Ce n'est qu'après vous être assuré de l'identité de votre interlocuteur que vous pourrez décider si vous désirez ou non répondre au questionnaire. Libre à vous également de ne pas répondre à l'une ou l'autre question en cours d'entretien.
Ne vous laissez pas abuser lorsque la participation ou les réponses à toutes les questions sont liées à un tirage au sort ou à un concours. Ces procédés vont à l'encontre de la bonne foi et sont illicites.

Attention!

- Pour vous informer de la finalité de l'utilisation de vos données, on utilise souvent la notion globale de "marketing". Or, celle-ci peut vouloir dire beaucoup: étude de marché, vente d'adresses, publicité...
  Demandez donc toujours la finalité exacte.
- Vu que les méthodes modernes de marketing ne sont en principe pas orientées uniquement sur un individu, mais sur un ménage, on vous demande la plupart du temps des informations relatives à vos colocataires, que ce soit par le biais de questionnaires ou de sondages par téléphone.
- Ne fournissez ce type d'informations qu'avec le consentement exprès de vos colocataires adultes. Quant aux indications concernant des enfants, ne les communiquez pas sans autre, même pas pour augmenter vos chances de gain à un concours. Car rien n'arrête la publicité: pas même les enfants!

Si vous avez d'autres questions à ce propos, n'hésitez pas à vous adresser au Préposé fédéral à la protection des données, 3003 Berne, tél. 031 / 322 43 95

6. Protection des données et collecte de dons, la feuille d'information du ZEWO

(ZEWO = Bureau central des œuvres de bienfaisance)

voir page 175

7. Qualification des données lors de la communication à l'étranger

voir page 180

8. Motion von Felten (98-3030). Droit de recours pour le Préposé fédéral à la protection des données

Mesdames, Messieurs,

Nous accusons réception de votre projet de réponse à la motion von Felten et vous en remercions. Par la présente, nous vous faisons part de notre avis.

Conclusions:

Nous ne sommes pas d'accord avec le projet de réponse et proposons au Conseil fédéral d'accepter la motion von Felten. Si notre proposition n'est pas suivie, nous vous prions de joindre la présente à la réponse du Conseil fédéral à l'adresse du Parlement.

Développement:

I.

1. Le Préposé fédéral à la protection des données (PFPD) est chargé de surveiller l'application par les organes fédéraux des dispositions fédérales relatives à la protection des données. A cette fin, il peut établir les faits et en cas de violation émettre des recommandations (art. 27 LPD). Il est également chargé de surveiller le respect de la protection des données par les personnes privées et d'établir les faits lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système), des fichiers doivent être enregistrés ou des communications à l'étranger doivent être déclarées. Au besoin, il peut recommander de modifier ou de cesser le traitement (art. 29 LPD). Le PFPD veille au respect de la personnalité et des droits et libertés fondamentaux de toutes personnes au sujet desquelles des données personnelles sont traitées par des organes fédéraux ou des personnes privées. Il exerce en particulier une fonction de conseil, de surveillance, d'information et de coordination (Regine Martina Sauter, Die institutionalisierte Kontrolle im Bundesgesetz über den Datenschutz vom 19. Juni 1992, Diss. St-Gallen, Zürich 1995, p. 109s.).

2. Les recommandations du PFPD n'ont pas de caractère contraignant. Toutefois lorsqu'un organe fédéral rejette ou ne suit pas une recommandation, le PFPD peut porter pour décision l'affaire auprès du département ou de la Chancellerie fédérale (art. 27, 4e al.). La décision doit alors être communiquée aux personnes concernées, lesquelles ont la possibilité de recourir à la Commission fédérale de la protection des données (art. 25, 5e alinéa LPD). Si la recommandation s'adresse à une personne privée et qu'elle est rejetée ou n'est pas suivie, alors le PFPD peut porter l'affaire devant la Commission fédérale de la protection des données qui décide (art. 29, 4e al. LPD). Contre la décision de la commission, le PFPD et/ou la personne privée peuvent recourir auprès du Tribunal fédéral.

3. La différence sur la marche à suivre lors du rejet ou du non respect des recommandations par les organes fédéraux ou par les personnes privées ne figurait pas dans le projet du Conseil fédéral du 23 mars 1988 (FF 1988 II 421ss). Elle a été, comme vous le soulignez dans votre projet de réponse, voulue par le Parlement qui estimait qu'il fallait laisser au chef du département concerné ou au chancelier de la Confédération une responsabilité politique sur les traitements effectués par ses services (cf. BO CE 1991, p. 1065; BO CN 1992, p. 389s et BO CE 1992, p. 228). Ce choix n'a pas été incontesté. En effet, le Conseil national soutenait le projet du Conseil fédéral, alors que le Conseil des États ne souhaitait pas donner au PFPD le droit de porter ses recommandations devant la commission et d'en requérir l'arbitrage. Dans le cadre de la procédure d'élimination des divergences, le chef du DFJP, Monsieur le Conseiller fédéral A. Koller a proposé, à titre de compromis, la solution finalement retenue (droit de porter la recommandation devant le département ou la Chancellerie).

II.

1. De lege lata, le PFPD n'a pas la possibilité de recourir contre une décision d'un département ou de la Chancellerie fédérale, même à titre exceptionnel comme l'a rappelé le TF dans son arrêt du 26 novembre 1997 (ATF 123 II 542ss). Cette situation n'est pas satisfaisante car comme le relève la Commission fédérale de la protection des données dans sa prise de position du 7 avril 1997 relative au recours du DFJP contre sa décision du 29 novembre 1996, "der EDSB hat wesentlich die Aufgabe, für die betroffenen privaten Personen in den komplexen öffentlichen oder privaten Datenbearbeitungen stellvertretend den Persönlichkeitsschutz zu sichern, weshalb er andere Interessen vertritt als die Departemente und die Bundeskanzlei."

2. Il est vrai qu'il n'est pas courant dans notre ordre juridique qu'une instance judiciaire tranche des conflits entre autorités d'une même collectivité publique. Cela n'est cependant pas exclu, et le législateur a envisagé cette possibilité (art. 48, lettre b de la loi fédérale du 20 décembre 1968 sur la procédure administrative qui légitime une autorité à recourir lorsque le droit fédéral l'autorise). Ainsi le PFPD s'est vu reconnaître la compétence de recourir contre les décisions de la Commission fédérale d'experts du secret professionnel en matière de recherche médicale (art. 32, 3e al. LPD). Il peut également requérir des mesures provisionnelles du président de la Commission fédérale de la protection des données "s'il constate à l'issue de l'enquête qu'il a menée en application de l'article 27, 2e alinéa ... que la personne concernée risque de subir un préjudice difficilement réparable" (art. 33, 2e al. LPD).

3. Il convient de souligner que le PFPD est un organe spécifique s'acquittant de ses tâches de manière autonome. Il n'est pas soumis à la surveillance d'un département ou de la chancellerie à laquelle il est rattaché administrativement. Le Conseil fédéral ne peut lui donner des instructions (Rolf Bründler, dans Maurer/Vogt (Hrsg.), Kommentar zum schweizerischen Datenschutzgesetz, Art. 26, N 12s.). Selon Sauter (op. cit., p. 108s.), le Conseil fédéral "hat sich dabei m.E. aber auf eine reine Dienstaufsicht über die Tätigkeit des Datenschutzbeauftragten zu beschränken und darf keine Rechtsmässigkeitskontrolle oder eine Kontrolle über Art und Weise der Erfülllung des Amtes aussüben." Or, en confiant au département ou à la chancellerie le soin de trancher entre le PFPD et un organe fédéral auquel il a adressé une recommandation, le PFPD est soumis à un contrôle de légalité par un organe qui est lui-même soumis à sa surveillance, ce qui est en contradiction avec son statut d'autonomie.

4. En outre, la protection des données concerne des biens juridiques élevés (droits et libertés fondamentaux, droits de la personnalité) et il se justifie, comme dans d'autres domaines du droit, de donner la possibilité au préposé fédéral de porter ses recommandations pour décision à une autre instance lorsqu'elles ne sont pas suivies ou qu'elles sont rejetées. Dans un avis du 14 février 1992 à l'intention de la Commission du CN chargée de l'examen du projet de loi fédérale sur la protection des données, l'Office fédéral de la justice note ce qui suit:

> "Bundesrat und Nationalrat möchten dem Datenschutzbeauftragten im öffentlichen Bereich eine Befugnis einräumen, die ihm im privaten Bereich nicht (mehr) bestritten wurde: Der Datenschutzbeauftragte soll auch im öffentlichen Bereich seine Empfehlungen der Datenschutzkommission zum Entscheid vorlegen können, wenn diese Empfehlungen von einer Bundesbehörde nicht befolgt werden. Prozessual gesehen kommt diese Befugnis einem Beschwerderecht des Datenschutzbeauftragten nahe, der den Erlass einer negativen Verfügung (das heisst einer Verfügung, die seiner Empfehlung zuwiderläuft) oder das Untätigsein einer Bundesbehörde nicht hinzunehmen braucht, sondern die Streitsache an eine obere (richterliche) Instanz weiterziehen kann. Der Ständerat stösst sich am Umstand, dass eine Bundesbehörde, wie sie auch der Datenschutzbeauftragte darstellt, gegen den Entscheid einer anderen Bundesbehörde ein Rechtsmittel ergreifen können soll. Solches widerspreche unserem Staatsverständnis...
>
> Aus rechtsdogmatischer Sicht lässt sich gegen die sog. "Insichprozesse" nichts einwenden, bei welchen in den gesetzlich umschriebenen Fällen eine Behörde den Entscheid einer anderen Behörde anfechten kann, auch wenn beide Behörden zur gleichen Gebietskörperschaft gehören... Es versteht sich von selbst, dass staatspolitische Verantwortung bei Prozessen zwischen Behörden Zurückhaltung gebietet. Es darf nicht der Eindruck entstehen, der Staat beschäftigte sich selber mit unnötigen Prozessen, oder politische Führungsverantwortung werde auf die Gerichte abgeschoben. In dieser Hinsicht ist dem Ständerat beizupflichten. Andererseits ist zu differenzieren: Aehnlich wie etwa beim Strahlenschutz sind beim Datenschutz

hochwertige Rechtsgüter betroffen. Es geht mitunter um äusserst empfindliche Eingriffe in die Persönlichkeitsrechte vieler Menschen. Gerade die Beurteilung der mit dem Schutz der Grundrechte zusammenhängenden Fragen ist in unserem Rechtsstaat zur eigentlichen "Gerichtstradition" geworden. Die Gerichte und vorab das Bundesgericht haben hier in verschiedener Hinsicht Pionierarbeit geleistet, wie es der Verwaltung nicht möglich gewesen wäre, die ja bekanntlich "von Amtes wegen" oftmals einer andere Optik haben muss. Es geht demnach beim Datenschutz und Grundrechtschutz nicht um ein Abschieben politischer Verantwortung, sondern vielmehr um die Zuweisung einer überaus heiklen Materie "an die richtige Adresse", wenn an einem gewissen Punkt die Gerichte eingeschaltet werden können. Das gilt sowohl für den privatrechtlichen als auch für den öffentlichrechtlichen Datenschutz, die sich bekanntlich an vielen Punkten überschneiden. Führt der Rechtsweg einheitlich über die Datenschutzkommission, kann die unbefriedigende Gabelung vermieden werden, die nach dem ständerätlichen Modell in jenen Fällen entstünde, wo sich (unabhängig vom Datenschutzbeauftragten) auch die direktbetroffenen Privaten gegen die Datenbearbeitung durch ein Bundesstelle zur Wehr setzen.

Der Datenschutzbeauftragte ist zwar Behörde, aber er wurde - und da hat man in der Schweiz Neuland betreten - als Ombudsmann konzipiert. Als solcher ist er nicht an Weisungen gebunden und soll (unter anderem) die Interessen der Bürger wahrnehmen, wo diese sich nicht oder nur ungenügend selber schützen können. Wenn die Behördenbeschwerde, die in der Schweiz ihren festen Platz hat, irgendwo Sinn macht, dann doch in erster Linie hier, wo in gewissen Bereichen nur der Datenschutzbeauftragte die Interessen unserer Bürger wirksam und umfassend vertreten kann. Zusammenfassend lässt sich daher sagen, dass sowohl von der Konzeption des Gesetzes als auch von der Natur der Sache her die Beschwerdelegitimation des Datenschutzbeauftragten als gerechtfertigt erscheint."

5. Le Préposé fédéral à la protection des données est avant tout un conseiller. Il n'a pas de pouvoir de décision, mais il peut émettre des recommandations. Certes, les personnes concernées ont la possibilité de recourir contre les décisions d'un département ou de la chancellerie. Toutefois, cette solution implique que la personne concernée soit suffisamment orientée sur les violations auxquelles le PFPD a recommandé de pallier. Si elle n'est pas elle-même intervenue dans la procédure, notamment en dénonçant une telle violation, il lui sera particulièrement difficile de faire usage de ses droits. Il lui faudra au préalable prendre connaissance du dossier, ce qui en présence de traitements complexes et dont le plus souvent elle ne connaissait pas l'existence, nécessite certaines connaissances que tout un chacun n'a pas. La personne concernée n'est en effet le plus souvent pas en mesure d'apprécier si un système d'informations est conforme à la protection des données ou s'il engendre des risques d'atteinte à sa personnalité. Cette appréciation est rendue d'autant plus difficile par la complexité et la technicité des systèmes. Tel est notamment le cas lorsqu'il s'agit d'apprécier les mesures de sécurité, la nécessité des accès aux données ou l'ampleur du traitement par rapport aux tâches à accomplir. Le Parlement a d'ailleurs reconnu cette difficulté en accordant au Préposé fédéral le droit dans le secteur privé de porter ses recommandations devant la commission fédérale de la protection des données et le droit de recourir contre les décisions de la Commission d'experts du secret médical en matière de recherche médicale.

6. A l'instar des décisions ZAR/AUPER, qui n'ont pas fait l'objet d'un recours des personnes concernées et pour lesquelles le TF a rejeté la légitimité du PFPD de recourir à la commission, l'absence de recours d'une personne concernée a pour conséquence qu'une recommandation rejetée par l'organe fédéral et par le département reste lettre morte, même si une violation des dispositions fédérales de protection des données existe (R. M. Sauter, op. cit., p. 130 qui considère qu'il y a là une lacune dans le système). Dans le cas ZAR/AUPER, la Commission fédérale de la protection des données avait admis dans sa décision annulée par le

TF (faute de légitimation pour la commission de statuer et pour le PFPD de recourir) des violations de la LPD. Il est vrai que le PFPD peut informer le Conseil fédéral (rapport d'activités ou rapport ad'hoc). Il peut également informer le public de ses constatations et recommandations lorsqu'il en va de l'intérêt général. Cela n'entraîne pas pour autant une élimination des lacunes constatées.

7. De plus, il n'est pas certain que le département concerné respecte la procédure en rendant une décision dans un délai raisonnable ou en informant les personnes concernées de la décision, en indiquant les voies de droit et les délais de recours. Ainsi, le DFI n'a jamais rendu de décision formelle sur notre recommandation du 15 décembre 1993 relative à la nouvelle liste des analyses (voir 1er Rapport d'activités du PFPD 1993/94, p.120). Le DFF n'a toujours pas rendu de décision sur la recommandation BV-Plus que nous lui avons transmise pour décision le 25 septembre 1996 (voir notamment 4ème Rapport d'activités 1996/97, p. 171s.). De même, le DETEC appelé à décider sur notre recommandation relative à l'affichage des numéros d'appel sur les appareils RNIS, n'a pas publié sa décision, ni mentionné les voies de droit et délai de recours.

8. Le système actuel ne permet pas de garantir la sécurité du droit par une pratique uniforme. En effet, le PFPD peut recommander certaines mesures sur la base de ses constatations et de son interprétation des dispositions légales. Un organe fédéral peut rejeter sa recommandation ou l'accepter. En cas de rejet le département ou la chancellerie tranche. Or chaque département appréciera le dossier selon sa sensibilité et ses intérêts, et il pourra en résulter sur des questions similaires ou identiques des décisions divergentes. En outre des questions d'interprétation du droit peuvent ainsi rester sans réponse. En accordant au PFPD, comme le propose la motionnaire, le droit de porter également ses recommandations à l'égard des organes fédéraux devant la Commission fédérale de la protection des données, on assure une plus grande homogénéité dans l'application du droit et une meilleure sécurité juridique.

9. Les traitements de données personnelles sur lesquels le PFPD est appelé à se prononcer et à émettre le cas échéant des recommandations sont souvent très complexes et concernent plusieurs organes fédéraux. Il n'est ainsi pas exclu que le département ou la chancellerie soit d'emblée impliqué par une recommandation du PFPD, soit parce qu'il est lui-même responsable ou co-responsable du traitement, soit parce que son conseiller à la protection des données, son responsable de la sécurité des données ou tout autre organe sont intervenus dans la réalisation du traitement ou du système d'information examinés par le PFPD. Dans de tels cas, le département, lorsqu'il est appelé à décider, se trouve dans la position de juge et partie.

10. Avec le transfert de certaines tâches publiques à des privés, avec la privatisation de certaines activités ou avec le mélange de certaines tâches légales avec des activités relevant du droit privé (par exemple, les caisses-maladie qui sont organe fédéral pour l'assurance obligatoire et personne privée pour l'assurance complémentaire facultative), la distinction entre organe fédéral et personne privée ne sera pas toujours aisée, et il est possible qu'une recommandation concerne en partie un organe fédéral et en partie un organe privé. Une telle situation n'est pas exclue dans le cadre de l'enquête relative au Natel. Cette imbrication des tâches publiques et privées justifie également une procédure identique.

11. La tendance en Europe et notamment au sein de l'Union européenne avec la directive 95/46/CE du 24 octobre 1995 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 va vers un renforcement des compétences des autorités chargées de surveiller l'application des dispositions de protection des données. La directive susmentionnée ne fait pas de distinction entre le secteur public et le secteur privé. Elle prévoit en particulier que ces autorités doivent pouvoir ester en justice en cas de violation des dispositions de protection des données (art. 28, chiffre 3).

9. Liste des 64 diagnostics de caractère général

(déductible automatiquement des codes "CIM-10" collectés à des fins statistiques dans les hôpitaux)

1. MALADIES INFECTIEUSES ET PARASITAIRES
   - organe (système) concerné

2. NEOPLASIES
   - néoplasies malignes, bénignes
   - organe (système) concerné

3. MALADIES DU SANG ET DES ORGANES HEMATOPOÏETIQUES AVEC CERTAINES DYSFONCTIONS EN RAPPORT AVEC LE SYSTEME IMMUNITAIRE

4. MALADIES ENDOCRINIENNES, DE LA NUTRITION ET DU METABOLISME
   - maladies de la thyroïde
   - diabète mellitus
   - maladies des autres glandes endocriniennes
   - troubles du métabolisme
   - troubles de l'équilibre acido-basique et du métabolisme de l'eau et des électrolytes

5. TROUBLES MENTAUX ET DU COMPORTEMENT

6. MALADIES DU SYSTEME NERVEUX
   - maladies inflammatoires du système nerveux central
   - affections extrapyramidales et troubles accompagnés de mouvements anormaux
   - maladies démyélinisantes du système nerveux central
   -épilepsie
   - migraine
   - AIT
   - affections des nerfs, du plexus nerveux et des racines
   - polyneuropathie
   - myasthénie
   - myopathie

7. MALADIES DE L'OEIL ET DE SES ANNEXES

8. MALADIES DE L'OREILLE ET DE L'APOPHYSE MASTOÏDE

9. MALADIES CARDIO-VASCULAIRES
   - hypertension artérielle
   - cardiopathies ischémiques
   - cor pulmonaire et troubles de la circulation pulmonaire
     (incl. embolie pulmonaire)
   - cardiopathie valvulaire
   - péricardite
   - myocardite
   - endocardite
   - cardiomyopathie
   - trouble du rythme cardiaque
   - insuffisance cardiaque
   - maladies cérébro-vasculaires
   - maladies vasculaires (incl. vasculite)

10. MALADIES DU SYSTEME RESPIRATOIRE

11. MALADIES DU SYSTEME DIGESTIF
    - maladies du système digestif haut

- maladies du système digestif inférieur
  (incl. maladie de Crohn, colites ulcèreuses)
- maladies du foie
- maladies de la vésicule biliaire, des voies biliaires, du pancréas

12. MALADIES DE LA PEAU ET DU TISSU SOUS-CUTANE

13. MALADIES DU SYSTEME MUSCULO-SQUELETTALE ET DU TISSU MOU
    - arthropathies
    - maladies des tissus conjonctifs p.ex. LE, dermatomoyosites
    - maladies de la colonne vertébrale et du dos
    - maladie du tissu mou
    - ostéopathies, chondropathies

14. MALADIES DES ORGANES URO-GENITAUX
    - affections rénales
    - urolithiasis
    - maladies des voie urinaires basses
    - affections génitales
    - affections du sein

15. GROSSESSE, ACCOUCHEMENT

16. CERTAINES AFFECTIONS DONT L'ORIGINE SE SITUE DANS LA PERIODE PERINATALE

17. ANOMALIES CONGENITALES, MALFORMATIONS ET ANOMALIES CHROMOSOMIQUES

18. SYMPTOMES, SIGNES ET ETATS MORBIDES, AILLEURS NON CLASSES
    - fièvre d'origine indéterminée

19. LESIONS TRAUMATIQUES ET EMPOISONNEMENTS

10. Recommandations du PFPD

10.1 Recommandation concernant la comparaison des données lors d'un examen de solvabilité

voir page 184