Préposé fédéral à la protection des données

Rapport d'activités 1996/97

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 1996 au 31 mars 1997.

TABLE DES MATIÈRES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

REPERTOIRE DES ABREVIATIONS

AI	Assurance-invalidité
AMA	Association suisse des assureurs privés maladie et accidents
ARCA	Association suisse des assureurs responsabilité civile et automobiles
AUPER	Système d'enregistrement automatisé des personnes
CEDH	Convention européenne des droits de l'Homme
CFPD	Commission fédérale de la protection des données
CI	Carte d'identité
CP	Code pénal suisse
DFAE	Département fédéral des affaires étrangères
DFEP	Département fédéral de l'économie publique
DFJP	Département fédéral de justice et police
ETV	L'annuaire téléphonique électronique de Télécom PTT
FMH	Fédération des médecins suisses (Foederatio Medicorum Helveticorum)
CdG	Commission de gestion du Conseil National
ISIS	Système de traitement des données relatives à la protection de l'Etat
JAAC	Jurisprudence des autorités administratives de la Confédération
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LDAu	Loi sur le droit d'auteur
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
LPD	Loi fédérale sur la protection des données
LREC	Loi fédérale sur la procédure de l'Assemblée (loi sur les rapports entre les conseils)
O DOSIS	Ordonnance sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants
OAMal	Ordonnance sur l'assurance-maladie
OC Stup	Office central de lutte contre le trafic illicite des stupéfiants
OFAS	Office fédéral des assurances sociales
OFEFP	Office fédéral de l'environnement, des forêts et du paysage
OFP	Office fédéral de la police
OFPER	Office fédéral du personnel
OLPD	Ordonnance relative à la loi fédérale sur la protection des donnéees
RAVS	Règlement sur l'assurance-vieillesse et survivants
RCE	Registre central des étrangers
RIPOL	Système de recherches de police
RNIS	Réseau numérique à intégration de services
ZEK	Centre d'informations de crédits

I. THEMES CHOISIS

1. Affaires de police

1.1. Loi sur les maisons de jeu

Dans le cadre de la consultation des offices, nous avons eu la possibilité de prendre position sur le projet de loi sur les jeux de hasard et sur les maisons de jeu (loi sur les maisons de jeu) ainsi que sur le message qui s'y rapporte.

L'Office fédéral de la police (OFP) nous a donné la possibilité, dans le cadre de la consultation des offices, de prendre position sur le projet de loi fédérale cité ci-dessus ainsi que sur le message qui s'y rapporte. La loi sur les maisons de jeu régit les conditions qui doivent être remplies pour exploiter un établissement de jeu. Pour des raisons d'ordre social ainsi que par intérêt propre les maisons de jeu sont autorisées à contrôler l'identité des joueurs et également dans certaines conditions à prononcer des interdictions de jeu et à accorder des crédits. Les maisons de jeu sont tenues de communiquer les interdictions de jeu prononcées à d'autres maisons de jeu. Lorsque il y a soupçon de blanchissage d'argent, celui-ci doit être communiqué au bureau de notification pour le blanchissage d'argent. Il est prévu de soumettre les maisons de jeu à la loi fédérale relative a la lutte contre le blanchissage d'argent dans le secteur financier. Selon cette loi, c'est l'Office central de lutte contre le crime organisé de l'Office fédéral de la police qui est chargé d'exploiter ce bureau de notification pour le blanchissage d'argent. Les différends existants en ce qui concerne la manière dont les maisons de jeu se procurent les informations et leur envergure en rapport avec l'imposition d'une interdiction de jeu ou l'accord de crédits, ainsi que sur le stockage et la suppression des données ont pu être réglés. En ce qui nous concerne, il nous reste à suivre le développement que prendra la soumission prévue des maisons de jeu à la nouvelle loi sur le blanchissage d'argent, et en rapport avec celle-ci, la communication de données au bureau de notification pour le blanchissage d'argent. Nous espérons également être impliqués aussi tôt que possible dans l'élaboration de l'ordonnance relative à la loi sur les maisons de jeu.

1.2. Connexion des cantons à ISIS

Pour venir à bout des tâches qui lui sont confiées, la Police fédérale suisse exploite le système de traitement des données relatives à la protection de l'Etat ISIS. A l'origine, il s'agissait d'un système isolé. Entre-temps et suite à une révision de l'ordonnance ISIS, des organes en provenance de neuf cantons y ont été reliés.

Conformément à l'ordonnance sur le système provisoire de traitement des données relatives à la protection de l'Etat (ordonnance ISIS), la Police fédérale suisse exploite un système provisoire de traitement des données relatives à la protection de l'Etat (ISIS) afin de pouvoir s'acquitter des tâches qui lui sont assignées de par la loi. A l'origine, ISIS était conçu comme système isolé. Bientôt le besoin se fit sentir auprès des organes de protection de l'État de procurer également aux organes cantonaux de protection de l'Etat un accès direct à ISIS. Par conséquent, en 1994 déjà, le Ministère public de la Confédération a envoyé le projet révisé de l'ordonnance ISIS en procédure de consultation auprès des offices, projet qui prévoyait un accès direct

à ISIS pour les organes cantonaux chargés de tâches liées à la protection de l'Etat fédéral. A cette époque déjà, nous avions saisi l'occasion de prendre position à ce sujet et avions soumis des propositions de modification concrètes. En 1996, lors d'une deuxième procédure de consultation, nous rendions attentif à notre prise de position précédente. Au niveau du contenu nos exigences

- pour une limitation des droits d'accès à un nombre restreint de cantons;
- pour une limitation des droits d'accès aux données d'identification de base (nom, prénom, organisation/raison sociale, pseudonyme, orthographie phonétique de tous les noms et prénoms, année de naissance, date de naissance, nationalité, lieu d'origine);
- pour une limitation des droits d'accès aux données concernant des événements ainsi qu'aux données de base complètes qui s'y réfèrent, auxquelles correspondent les informations obtenues auprès de l'organe concerné ou qui ont été communiquées à ce dernier par la Police fédérale;
- demandant de renoncer à un accès à la base de données «Documentation»

on été remplies.
Entre-temps, cette affaire a été interrompue suite à des querelles de compétence entre la Police fédérale suisse et l'Office fédéral de la police. Il semble ne pas être clair, lequel de ces deux offices est responsable pour le domaine du crime organisé.

1.3. Le système de traitement de données DOSIS

Accès en ligne aux données DOSIS

L'Office central de lutte contre le trafic illicite des stupéfiants (OC Stup) de l'Office fédéral de la police (OFP) dispose pour sa lutte contre le trafic illicite des stupéfiants du système de traitement de données DOSIS. Le nombre de personnes ayant accès en ligne aux données personnelles stockées dans DOSIS est trop élevé.

Conformément à la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC), l'Office fédéral de la police (OFP) dirige l'Office central de lutte contre le trafic illicite des stupéfiants (OC Stup). L'OC Stup dispose selon l'ordonnance sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants (ordonnance DOSIS) du système de traitement de données DOSIS. L'ordonnance DOSIS stipule expressément que seul l'OC Stup ainsi que les services des stupéfiants des corps cantonaux de police peuvent être reliés au système DOSIS pour consulter des données. L'annexe 2 de l'ordonnance DOSIS étend cependant les droits d'accès, en contradiction avec la loi, en autorisant un accès aux collaborateurs de l'OFP qui ne font pas partie de l'OC Stup. Par lettre, nous avons rendu attentif l'OFP à cet état de fait et l'avons invité à respecter nos exigences lors des traitements de données dans DOSIS.
Il y a lieu dans ce cadre d'examiner si une révision de la LOC et de l'ordonnance DOSIS doit être entamée afin de pouvoir tenir compte des problèmes résultant des tensions qui existent dans le domaine crime organisé/trafic des stupéfiants.

Règlement de traitement DOSIS

Conformément à l'ordonnance relative à la loi fédérale sur la protection des données (OLPD), les organes fédéraux qui détiennent des fichiers automatisés sont, dans

certaines conditions, tenus d'élaborer un règlement de traitement. L'office fédéral de la police (OFP) a élaboré le règlement de traitement pour le système DOSIS.

Conformément à l'OLPD, les organes fédéraux qui détiennent des fichiers automatisés doivent élaborer un règlement de traitement lorsque le fichier contient des données sensibles ou des profils de la personnalité, lorsque le fichier est utilisé par plusieurs organes fédéraux, lorsqu'un accès est offert aux cantons, à des autorités étrangères, à des organisations internationales ou à des personnes privées ou lorsque le fichier est relié à d'autres fichiers. Le 1er août 1996, le système de traitement des données DOSIS a été définitivement mis en service. Son exploitation nécessitait un règlement de traitement DOSIS de la part de l'OFP. Nous avons collaboré avec l'OFP pendant la phase d'élaboration dudit règlement. Ceci nous a permis de rendre attentif à certains aspects problématiques, voire inadmissibles du point de vue de la protection des données. Malheureusement, les divergences n'ont pas pu être réglées en ce qui concerne un point essentiel: conformément à l'ordonnance DOSIS, les services des stupéfiants des corps cantonaux de police sont également directement reliés à DOSIS en plus de l'OC Stup. A notre avis, le règlement de traitement élaboré par l'OFP élargit de manière illicite le cercle des personnes autorisées à accéder au système. Le règlement de traitement prévoit que des collaborateurs des corps de police qui ne font pas partie du service des stupéfiants peuvent être reliés à DOSIS afin de remplir leurs tâches légales. Nous sommes d'avis que l'ordonnance DOSIS ne contient aucune base légale permettant un tel élargissement des possibilités d'accès. L'application pratique du règlement de traitement serait ainsi contraire à la loi.
Nous tenons en outre à relever que ce règlement et ses annexes est un ouvrage volumineux pour l'élaboration duquel l'OFP s'est donné beaucoup de peine.

Séparation des données collectées avant l'ouverture d'une procédure d'enquête de police judiciaire de celles de la police judiciaire de la Confédération et des cantons dans DOSIS.

Le système de traitement de données DOSIS pour la lutte contre le trafic illicite de stupéfiants traite aussi bien des données obtenues dans le cadre d'une procédure d'enquête de police judiciaire que des données qui existaient déjà avant que cette procédure soit engagée. Selon la loi fédérale sur les Offices centraux de police criminelle de la Confédération, ces données doivent être gérées séparément.

L'Office central de lutte contre le trafic illicite des stupéfiants (OC Stup) de l'Office fédéral de la police (OFP) utilise le système de traitement de données DOSIS pour la lutte contre le trafic illicite des stupéfiants. Ce système mémorise et traite d'une part des données personnelles obtenues avant l'ouverture d'une procédure d'enquête de police judiciaire, d'autre part des données appartenant aux polices judiciaires de la Confédération et des cantons.
La loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) stipule que ces données doivent être gérées séparément dans DOSIS. Dans un système de traitement de données, une telle séparation peut être faite de manière logique ou physique. Nous avons pour l'instant renoncé à demander une séparation physique, c.-à-d. la gestion de deux bases de données. DOSIS cependant ne procède même pas à la séparation logique obligatoire des données, les données étant affichées sur un écran commun avec la mention «PolJu oui/non». Nous avons informé l'OFP par lettre que la situation actuelle était contraire à la loi et

avons demandé que le traitement des données dans DOSIS soit adapté selon nos déclarations.
L'appréciation de la question de savoir s'il s'agit de données obtenues avant l'ouverture d'une procédure d'enquête de police judiciaire, ou s'il s'agit de données appartenant aux polices judiciaires cantonales se fait sur la base des codes de procédure pénale cantonaux qui sont parfois très divergents. Selon les cantons, cet état de fait peut mener à une inégalité de traitement et poser des problèmes de faisabilité.

Droit d'accès indirect dans DOSIS

Le droit d'accès du citoyen quant à un enregistrement éventuel dans le système de traitement des données DOSIS se distingue fortement du droit d'accès prévu par la LPD: il s'agit d'un droit d'accès indirect devant être exercé par le biais du Préposé fédéral à la protection des données.

La LPD prévoit un droit d'accès permettant à toute personne de demander au maître d'un fichier si des informations concernant sa personne sont traitées. La personne concernée adresse sa demande directement au maître de fichier.
Conformément à l'ordonnance DOSIS, la personne concernée ne peut s'adresser directement au maître de fichier que dans les cas ou la procédure d'enquête de police judiciaire a été menée par la Confédération. En revanche, lorsqu'il s'agit de données collectées avant l'ouverture d'une procédure d'enquête de police judiciaire ou qui dépendent des polices judiciaires des cantons, c'est le droit d'accès indirect qui est applicable, comme nous l'avons déjà expliqué dans notre 2ème rapport d'activités aux pages 102 ss. Celui-ci est régi par les dispositions de la loi fédérale sur les Offices centraux de police criminelle de la Confédération, qui dévie de manière substantielle des dispositions de la LPD. Conformément à ces dispositions, la personne concernée doit s'adresser à nous pour nous demander si des données sont traitées dans DOSIS de manière licite. Dans tous les cas, notre réponse à la personne requérante est soit qu'aucune donnée la concernant n'est traitée de manière illicite, ou dans les cas ou une erreur de traitement existe, que nous avons adressé une recommandation à l'OC Stup pour corriger cet état de fait. Ce droit d'accès indirect ne peut être satisfaisant pour la personne concernée et est simplement inadmissible en ce qui nous concerne. La personne concernée ne reçoit pas de réponse claire à la question de savoir si des données la concernant sont traitées et le cas échéant lesquelles. Pour nous, ce droit d'accès indirect nécessite d'une part que nous vérifions dans le système de traitement de données DOSIS si et le cas échéant quelles données concernant la personne requérante sont traitées. D'autre part, nous devons étudier les dossiers, en partie sur support papier, parfois volumineux, et ne concernant souvent pas une seule personne mais des opérations entières, pour pouvoir évaluer si la saisie et le traitement des données dans DOSIS ont été effectués de manière licite. Afin de pouvoir vérifier la justesse et/ou la licéité du traitement des données, nous devrions obtenir et traiter nous-mêmes des données sur la personne requérante. Nous deviendrions ainsi nous-mêmes des maîtres de fichiers. Cette approche ne serait cependant pas compatible avec la tâche qui nous a été confiée par la loi et qui consiste à exercer une fonction de surveillance. En 1996, une seule demande d'accès indirect nous a été adressée.

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

Un CD-ROM contenant des données sur les détenteurs de véhicules à moteur de toute la Suisse (à l'exception du canton du Jura) a été mis en vente. Un tel acte enfreint les dispositions de la loi sur la protection des données et de la législation sur la circulation routière. Nous avons finalement émis une recommandation demandant de cesser la production et la diffusion de ce CD-ROM.

Divers organes cantonaux de protection des données et les autorités de la circulation routière ont attiré notre attention sur le fait qu'un CD-ROM contenant un annuaire des détenteurs de véhicules à moteur était diffusé. Nous avons demandé à l'entreprise responsable de cette diffusion de suspendre la production et la vente de ce CD-ROM jusqu'à ce que l'état de faits soit éclairci. Cette dernière nous a confirmé qu'elle avait cessé la production et la vente et a également répondu à nos questions par écrit. Après avoir éclairci les faits, il s'est avéré que l'exactitude des données n'était pas garantie et que les options de recherche offraient des possibilités de consultation de données trop poussées. Nous avons en outre constaté que les données avaient été reprises des annuaires cantonaux des détenteurs de véhicules à moteur pour être publiées sous forme de CD-ROM.
La législation sur la circulation routière autorise la recherche et la communication du nom et du prénom d'un détenteur de véhicule uniquement sur la base du numéro d'immatriculation. Le législateur a ainsi manifesté sa volonté de limiter à un minimum les possibilités de traitement des données se rapportant à des détenteurs de véhicules à moteur afin d'éviter que de graves atteintes à la personnalité d'un détenteur puissent en résulter. Le CD-ROM dont il est question ici permettait cependant des recherches selon une multitude de critères (tels que nom, commune, numéro postal d'acheminement, plaque d'immatriculation) ce qui correspondait à des possibilités de recherche quasi illimitées. Une telle démarche touchait non seulement la législation sur la circulation routière, mais également le principe de proportionnalité en matière de protection des données. Conformément aux dispositions de la loi sur la circulation routière applicables en la matière, le traitement de données se rapportant à des détenteurs de véhicule est réservé à la Confédération. Dans ce cadre, elle traite et publie ces données à des fins qui sont en rapport direct avec l'accomplissement des tâches prévues par la législation sur la circulation routière, en particulier avec les tâches de police. La diffusion des données concernant des détenteurs de véhicules à moteur représente par contre une activité commerciale qui n'a aucun rapport avec les objectifs de la législation sur la circulation routière.
En outre, ce procédé viole non seulement les règles de compétence existantes, mais également le principe de finalité. En diffusant des données qui ont été mal numérisées et qui partiellement ne sont pas à jour, on ne respecte en outre pas l'exigence de l'exactitude. Nous avons finalement recommandé de cesser définitivement la production et la diffusion de ce CD-ROM.

1.5. Casier judiciaire entièrement automatisé VOSTRA

Il est prévu d'automatiser ce registre qui jusqu'ici est tenu sous forme de papier (projet VOSTRA). Un casier judiciaire traite entre autres des données sensibles. Il est donc nécessaire de créer la base légale requise - une loi au sens formel - pour ce

nouveau système. Actuellement, un projet pilote est en cours avec quelques cantons, il se termine fin 1998.

La section casier judiciaire de l'Office fédéral de la police tient un registre concernant toutes les personnes qui on subi une condamnation sur le territoire de la Confédération, ainsi que sur tous les citoyens suisses ayant été condamnés à l'étranger. L'automatisation de ce registre devrait permettre une gestion plus efficace des extraits de jugements et du casier judiciaire. Selon la loi sur la protection des données, le projet VOSTRA qui contient des données sensibles accessibles par procédure d'appel (online) doit être prévu dans une loi au sens formel.
Une courte visite auprès de l'Office fédéral de la police a montré que le casier judiciaire sous sa forme actuelle n'est plus en mesure de remplir de manière satisfaisante les tâches qui lui sont assignées par la loi. Nous avons donc consenti à la modification de l'ordonnance sur le casier judiciaire posant les bases pour lancer un essai pilote avec neuf cantons ainsi qu'avec l'Office de l'auditeur en chef de l'armée. Cette ordonnance est valable jusqu'à fin 1998. L'Office fédéral de la police s'est en outre engagé à créer d'ici au 31 décembre 1998 les bases légales au sens formel nécessaires pour une exploitation efficace du système VOSTRA. L'ordonnance relative au casier judiciaire devra alors faire l'objet d'une révision totale.

2. Droit des étrangers et droit d'asile

2.1. Accès des organes de police aux fichiers du DFJP sur les requérants d'asile et les étrangers - décision de la CFPD

Suite à nos recours, la CFPD a annulé les décisions du DFJP et a renvoyé la cause à l'instance inférieure pour être jugée à nouveau. Dans sa décision, la CFPD a tiré au clair quelques aspects importants de la protection des données et a également donné son avis sur notre droit de recours. Le DFJP a déposé un recours de droit administratif contre cette décision auprès du Tribunal fédéral. Ainsi, ce conflit juridique entre maintenant dans sa 5ème année déjà.

Dans un rapport de sécurité de 1992, ainsi que dans deux recommandations de 1994, nous nous sommes exprimés contre le stockage et le traitement en commun des données concernant les requérants d'asile et les étrangers avec des données pénales. Nous avons en outre demandé que les différentes autorités de police de la Confédération ne disposent pas - depuis les moyens informatiques utilisés - d'accès online aux données sensibles des requérants d'asile et des étrangers, sans qu'il y ait pour cela une base légale suffisante et sans que les problèmes de sécurité aient été suffisamment étudiés. Il s'agissait plutôt de stopper, respectivement de restreindre à un minimum les accès existants selon le principe du self-service avec son danger inhérent de fuites de données incontrôlées.
Les offices concernés ainsi que le DFJP rejetèrent nos recommandations et nos recours, de sorte que nous fûmes obligés de recourir auprès de la Commission fédérale de la protection des données (CFPD). La CFPD accepta nos recours dans une grande mesure, annula les dispositions contestées du DFJP et renvoya la cause pour nouvelle décision au DFJP.
Dans sa décision, la CFPD reconnut le droit de recours du PFPD contre les décisions des départements et de la Chancellerie fédérale, dans les cas ou les décisions de ces autorités entravent fortement l'exercice des activités du PFPD. En ce qui

nous concerne, nous avions défendu le point de vue selon lequel notre droit de recours contre ces organes fédéraux découlait de notre statut autonome au sein de l'Administration fédérale et était fondée directement sur la loi fédérale sur la procédure administrative. Ceci expliquait qu'il n'était pas explicitement mentionné dans la loi sur la protection des données. D'autre part, la CFPD estima que les bases légales pour les accès online contestés étaient clairement insuffisantes, en tous les cas au moment où le recours avait été déposé. La CFPD a en outre retenu que des mécanismes de journalisation des accès auraient dû être mis en place, permettant d'établir des protocoles efficaces. Elle défendit le point de vue que notamment les données concernant des requérants d'asile et dans ce contexte aussi la nationalité étaient des données sensibles, que d'autre part, les données se rapportant à des personnes qui n'étaient pas impliquées dans une procédure ne devaient pas être accessibles online, qu'en général les données des requérants d'asile et des étrangers devaient être stockées et traitées séparément des données pénales. Du point de vue formel, la CFPD demanda que les nouvelles décisions à prendre par le DFJP soient publiées intégralement dans la Feuille fédérale. Les décisions contestées n'avaient en fait été publiées que sous une forme très abrégée et ceci uniquement après notre intervention.
Le DFJP a déposé un recours de droit administratif contre la décision de la CFPD auprès du Tribunal fédéral.

2.2. Le projet EVA (délivrance automatisée de visas)

Les représentations suisses à l'étranger ainsi que les plus importants postes frontières de Suisse délivrent de tout temps déjà des visas. Dans ce cadre, ils sont tenus entre autres de vérifier l'exactitude des données fournies par les requérants. Le projet EVA devrait permettre, avant l'établissement du visa, la consultation électronique des fichiers existants et de ceux qui seront encore créés à l'avenir ainsi que l'impression automatisée des visas. Se posent les questions de savoir comment les traitements de données, notamment ceux effectués à l'étranger, peuvent être suffisamment protégés et si les bases légales sont suffisantes pour les nouveaux et nombreux traitements de données prévus.

A l'occasion de deux contrôles effectués en 1996 (voir aussi p. 174 ci-après), nous avons eu un bon aperçu des traitements de données effectués lors de l'établissement des visas dans les représentations suisses à l'étranger ainsi qu'aux postes frontières. Ces autorités délivrent les visas de manière manuelle après avoir consulté le Moniteur suisse de police et, en cas de doute, l'Office fédéral des étrangers, qui procède à des recherches complémentaires. Les postes de contrôle frontières disposent depuis peu de temps d'un accès (restreint) au système de recherches RIPOL, au Registre central des étrangers RCE et désormais également aux données concernant les requérants d'asile disponibles dans AUPER. Les représentations suisses à l'étranger par contre ne disposent pas de tels accès (à l'exception de quelques grandes ambassades qui ont un accès direct au système RIPOL). Des comportements abusifs de la part des requérants (tels que le dépôt d'une demande de visa dans plusieurs consulats ou auprès de plusieurs postes frontières), les temps d'attente lorsque des recherches complémentaires doivent être faites à Berne ainsi que le désir de disposer d'un instrument de travail convivial au guichet ont mené à l'idée du projet pour l'établissement automatisé des visas. Le projet a traversé la phase de l'analyse préliminaire et se trouve actuellement dans la phase de conception. En ce qui concerne la protection des données, nous avons

suggéré d'étudier si les ambassades et consulats suisses avaient vraiment absolument besoin dans tous les cas de consulter les fichiers sensibles RIPOL, RCE et AUPER, et si le fait que les visas étaient délivrés sur place par du personnel étranger ne présentait pas de risques. De manière générale, nous avons proposé une évaluation des risques selon les directives applicables ainsi que l'élaboration d'un concept de sécurité. Un facteur de risque particulier pourraient être les réseaux locaux des représentations suisses à l'étranger, qui permettraient d'intercepter les accès online ou qui pourraient être utilisés par des organisations criminelles pour accéder aux fichiers sensibles stockés en Suisse. Nos suggestions ont été bien reçues. Un contrôle a établi que des recherches complémentaires n'étaient nécessaires que pour 5% des demandes de visa. Il suffit donc dans 95% des demandes que ce soit le système (évidemment dans un environnement sûr), et non pas l'employé au guichet, qui lance une recherche dans les fichiers intéressés pour ensuite simplement retransmettre un «message OK» à la représentation suisse à l'étranger. Pour les 5% de cas restants, la demande sera envoyée à Berne, comme c'est le cas aujourd'hui. Cette démarche permet d'éviter les consultations online problématiques.
Dans un avis de droit conséquent, nous avons d'autre part exprimé notre avis sur la question des bases légales. Nous sommes arrivés à la conclusion que pour certains aspects isolés des nouveaux traitements de données prévus, les bases légales existantes suffisent ou ont déjà été proposées au Parlement (voir aussi p.136 ci-après). L'idée de projet telle qu'elle est soumise aujourd'hui nécessiterait cependant une déclaration de principe claire dans la loi sur le séjour et l'établissement des étrangers, disposition qui fait actuellement défaut et qui n'est pas non plus prévue. Dans ce contexte, il y a lieu de tenir compte du fait qu'il est prévu de créer un nouveau fichier volumineux qui enregistre tous les mouvements de personnes en rapport avec un visa ainsi que les attributs qui s'y rapportent et les mémorise pour une longue durée. Lors de la délivrance d'un visa, ces données sont traitées en même temps que les données en provenance d'autres gros fichiers, et par conséquent nombre d'autorités vont accéder régulièrement à ces données, qui sont en partie des données sensibles.

2.3. Concept global de sécurité pour les accès des cantons au RCE

La question de la sécurité globale dans les rapports entre la Confédération et les cantons se pose également lors du traitement électronique des données relatives aux étrangers. Beaucoup de cantons ont accepté d'adopter les exigences de sécurité de la Confédération. En ce qui concerne un autre canton, nous sommes actuellement en discussion avec les spécialistes de la sécurité de la Confédération.

Dans un avis de droit publié dans la JAAC 60.10, nous nous sommes exprimés vers la fin de 1994 déjà sur les conditions prévues par le droit fédéral pour le traitement de données se rapportant à des étrangers auprès de la Confédération et des cantons. Le Registre central des étrangers RCE est également à la disposition des autorités cantonales dans la mesure où ceci est nécessaire pour l'accomplissement des tâches de ces dernières et compatible avec le but dans lequel les données avaient été collectées à l'origine. Aucun autre traitement de données n'est autorisé. Tous les utilisateurs du RCE doivent garantir que les données du RCE ne sont pas utilisées à d'autres fins ou que des tiers non autorisés peuvent accéder aux données du RCE et soustraire ou modifier des données. Il paraît donc évident qu'il y a lieu de

choisir une norme de sécurité commune très élevée. La sécurité au sein du RCE engage la coresponsabilité de chaque utilisateur. Les cantons qui désirent déléguer les droits d'accès au RCE à un grand nombre de leurs propres autorités doivent veiller à ce que tous les utilisateurs remplissent la norme de sécurité exigée. Étant donné que la sécurité engendre aussi des coûts, nous conseillons de créer des structures d'organisation économes et si nécessaire de les alléger. Cette démarche s'inscrit dans l'optique du New Public Management et a déjà été adoptée par un grand nombre de cantons. En ce qui concerne un autre canton, nous avons analysé la situation avec les spécialistes de la sécurité de la Confédération de manière à ce que les mesures de protection et de sécurité nécessaires puissent être prises avant que de nouveaux accès au RCE soient installés.

2.4. Les mentions «à la recherche d'un emploi» et autres sur les livrets d'étranger

Étant donné que le livret d'étranger sert aujourd'hui aussi de décision, il contient un certain nombre d'indications qui n'ont rien à voir avec l'identité d'une personne. Une base légale pour de telles «pièces d'identité» fait défaut, ce qui n'est pas satisfaisant du point de vue de la protection des données.

Un ressortissant étranger s'est plaint auprès de nous que son livret d'étranger comportait entre autres les mentions «à la recherche d'un emploi» et «attendant une décision de rente». Selon les indications fournies par les autorités de police des étrangers, de telles mentions sont conformes à la pratique. Entre-temps, l'autorité compétente a cependant décidé elle-même de supprimer la mention «attendant une décision de rente» dans le livret. Par contre, elle n'a pas voulu renoncer à la mention «à la recherche d'un emploi». Elle justifia ceci par le fait que selon elle le livret d'étranger ne représentait pas seulement une pièce d'identité, mais également une décision en ce qui concerne le droit de résidence de l'étranger; que cet acte devait donc clairement indiquer les motifs et conditions exigés par la loi qui justifient le séjour en Suisse; que le fait de délivrer une décision séparée en plus du livret d'étranger proprement dit représenterait une grosse charge de travail supplémentaire. Cette justification ne nous a pas convaincus. La charge de travail administratif supplémentaire pourrait être compensée par des émoluments et elle pourrait sans autre être prise en charge par les systèmes automatisés de dactylographie déjà existants dans la majorité des services. D'autre part, pour une décision, il manque la rubrique «voies de recours». On ne s'est pas non plus efforcé de masquer le dispositif. Ceci signifie que chaque présentation de ce document rend automatiquement visibles des informations assez poussées sur la situation personnelle du porteur. Il n'existe pas de base légale justifiant ceci et la législation en matière de protection des données s'oppose à une telle pratique. Nous avons fait part des ces constatations aux autorités compétentes. Sous forme de mesure immédiate, l'Office fédéral des étrangers s'est déclaré prêt à restreindre la liste des mentions prévues pour les livrets d'étrangers. Il sera pourtant nécessaire d'aborder le problème de manière fondamentale dans le cadre des travaux pour une nouvelle législation en matière de migration.

2.5. La communication de données concernant des requérants d'asile à des Etats étrangers

Il n'est pas autorisé de communiquer les empreintes digitales de requérants d'asile à l'étranger, si un tel acte est susceptible de mettre gravement en danger la personnalité des personnes concernées. Pour la communication de données aux autorités d'asile des pays de l'UE disposant d'une protection des données équivalente à la nôtre, nous n'avons pas vu ce danger. Nous avons cependant dû refuser deux autres communications de données à l'étranger après avoir étudié les faits.

Dans un avis de droit publié dans la JAAC 60.89, nous nous sommes exprimés sur la question de la communication de données concernant des requérants d'asile à des Etats étrangers. En l'occurrence, il s'agissait des trois cas concrets suivants:

- la communication des empreintes digitales à l'état d'origine pour l'exécution d'une décision de renvoi;
- la communication aux autorités d'asile d'un état européen pour déterminer le pays de premier asile;
- la communication à des services Interpol étrangers à des fins policières.

Conformément au principe de «non-refoulement» découlant de la CEDH, personne ne doit être soumis à la torture ou à une peine ou un traitement dégradants. Selon la législation de la CEDH, cette disposition interdit également l'expulsion ou l'extradition vers un pays dans lequel il faut s'attendre à ce que la personne soit torturée ou soumise à un traitement inhumain ou dégradant. Elle ne s'applique pas seulement aux réfugiés, mais aussi aux délinquants qui sont extradés. Ce principe a été repris et commenté dans diverses dispositions du droit fédéral, notamment dans la loi sur l'asile, dans la loi sur l'entraide judiciaire et désormais aussi - avec le principe constitutionnel de la liberté individuelle, respectivement de la protection de la personnalité - dans la loi sur la protection des données. Selon l'article 6 de cette dernière des données personnelles ne doivent pas être communiquées à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse.

En tenant compte de toutes ces bases légales, nous sommes arrivés à la conclusion suivante dans ces trois cas: la communication d'empreintes digitales à un pays qui viole gravement les droits de l'Homme, qui de surcroît possède les empreintes digitales de tous ses citoyens et qui poursuit de manière acharnée les personnes simplement soupçonnées d'être hostiles au régime, est considérée comme pouvant porter gravement atteinte à la personnalité de la personne concernée. Ceci est notamment le cas si l'on peut soupçonner que déjà la communication des empreintes digitales mène à une «mise en suspicion» politique et pourrait générer des traitements de données diffamatoires et discriminatoires. Dans le cas concret, il faudrait prouver qu'une garantie suffisante pour une bonne protection des droits de l'Homme (y compris la protection de la personnalité) peut être donnée. Les mêmes raisonnements ont guidés le Tribunal fédéral, pour autant que cela soit visible, dans un cas d'extradition récemment traité (voir ATF 122 II 373). Elles s'appliquent également à l'échange de données entre les autorités d'enquêtes et les autorités pénales internationales. Par contre, nous n'avons pas vu d'atteinte grave à la personnalité des personnes concernées lors de l'échange de données concernant des requérants d'asile entre autorités d'asile des pays européens ayant une protection des données équivalente.

2.6. Contrat entre les Archives fédérales et Yad Vashem sur la communication de données relatives à des réfugiés juifs

Yad Vashem, une collectivité de droit public en Israël, qui défend les intérêts des survivants de l'holocauste et représente les familles des victimes, a prié les Archives fédérales de leur communiquer les données de réfugiés juifs entre 1933 et 1945.

Les Archives fédérales ont donné leur accord à cette communication. Elles nous ont soumis un projet de contrat et nous ont montré les fichiers concernés. Nous avons proposé d'y intégrer les dispositions nécessaires selon la législation suisse en matière de protection et de sécurité des données. Selon ces dernières, des recherches dans l'intérêt des réfugiés juifs ou de leurs familles ou descendants peuvent également être faites en Israël. En même temps, leurs données personnelles sont protégées contre tout traitement illicite.

2.7. Consultation du PFPD concernant la révision en cours de la loi sur l'asile et de la loi sur les étrangers

La commission d'examen préalable du Conseil national nous a invité à prendre position sur les dispositions de protection des données contenues dans les deux projets de révision.

A cette occasion, nous avons été priés de commenter plus en détail l'opinion que nous avions défendue dans nos précédents rapports d'activités (voir en dernier: 3ème rapport d'activité 1995/96 p. 129 ss). Nous avons expliqué une nouvelle fois que la communication de données personnelles à l'étranger aussi selon l'article 6 LPD ne doit pas mener à une mise en danger grave des personnes concernées ou de leurs proches. Si l'Etat destinataire ne dispose pas d'une loi sur la protection des données équivalente à celle en vigueur en Suisse, des garanties doivent pouvoir être données pour la protection des données et de la personnalité des personnes concernées au moyen d'accords spécifiques ou d'autres mesures. Nous ne considérons pas de tels accords comme étant des «accords sans importance». De manière générale, nous avons proposé dans ce contexte d'étudier la question de savoir dans quels cas le Parlement devait conclure ou approuver des accords internationaux dans le domaine de la migration. Nous avons également considéré comme problématique la pratique actuelle qui consiste à prendre les empreintes digitales de tous les requérants d'asile et de communiquer ces données aux pays d'origine. Nous avons proposé d'étudier des solutions qui n'iraient pas si loin. De nouvelles recherches ont montré que seule une infime partie des requérants d'asile présente abusivement des demandes en double (voir p. 171 ci-après) et qu'il est relativement facile d'établir des prévisions à ce sujet.
Conformément à notre enquête interne auprès de divers délégués à la protection des données d'autres pays, le fait de prendre les empreintes digitales de tous les requérants d'asile sur l'ensemble du territoire ne correspond pas du tout à une pratique générale en Europe. Plusieurs pays européens ne prennent les empreintes digitales des requérants d'asile que dans les cas où il y a un soupçon de comportement abusif. Il n'y a pas de raison s'opposant à ce que notre pays opte pour une telle solution. Il faudrait bien sûr prévoir une certaine marge de manoeuvre pour le Conseil fédéral pour le cas où - contrairement à nos attentes - des changements interviendraient prochainement en Europe à la suite de nouveaux accords multinationaux, démarche que nous pourrions alors accepter. Nous avons

une nouvelle fois rendu attentif au fait que la communication de données en provenance des fichiers sensibles des requérants d'asile et des étrangers ne peut se faire par procédure d'appel que si ceci est absolument *indispensable* à l'exécution des tâches légales.

2.8. Prolongation de l'arrêté fédéral sur la procédure d'asile

Etant donné que l'arrêté fédéral sur la procédure d'asile arrive à échéance avant la révision totale de la loi sur l'asile, il doit être prolongé par les Chambres fédérales. Celles-ci ont ainsi une possibilité élégante de mettre immédiatement en vigueur les nouvelles dispositions de protection des données pratiquement «prêtes» de la loi révisée sur l'asile qui ne sont pas contestées sur leur principe. Nous trouvons qu'il ne serait par contre pas indiqué d'attendre d'ici l'an 2000, surtout en tenant compte du fait que la LPD a fixé le délai pour émettre de telles dispositions de protection des données au 1er juillet 1998.

A l'occasion de la prolongation de l'arrêté sur la procédure d'asile, nous avons proposé dans le cadre de la procédure de consultation des offices, de mettre en vigueur les nouvelles dispositions de protection des données pratiquement «prêtes» de la loi révisée sur l'asile, qui sur leur principe ne sont pas contestées, directement au moment de la prolongation de l'arrêté. Nous étions d'avis qu'il n'était pas opportun d'attendre que la loi révisée sur l'asile soit mise en vigueur en 1999 ou même plus tard, étant donné que l'article 38, 3e alinéa, de la loi sur la protection des données (LPD) exige que les dispositions de protection des données qui manquent dans les lois au sens formel doivent être édictées d'ici le 1er juillet 1998.
Cependant le Conseil fédéral a proposé une autre solution au Parlement, ceci sans nous avoir consulté une nouvelle fois dans le cadre de la procédure de consultation. Cette solution prévoit de prolonger le délai d'adaptation pour le domaine de l'asile au 31 décembre 1999 moyennant un nouvel alinéa 4 à l'article 38 LPD.
Nous sommes cependant d'avis qu'il existe aujourd'hui déjà un nombre de traitements de données délicats dans le domaine de l'asile pour lesquels il n'existe pas de base légale suffisante et qui ne sont pas non plus régis par les dispositions transitoires de l'article 38 LPD. La Commission fédérale de protection des données semble partager ce point de vue dans sa décision du 29 novembre 1996 (voir p. 131 ci-devant). D'autre part, le Tribunal fédéral a récemment contraint une autorité cantonale par un jugement qui a été très suivi de détruire des données sensibles que celle-ci avait collectées sans base légale suffisante. Ceci présente donc un danger considérable pour les autorités d'asile si les bases légales manquantes ne sont pas rapidement créées. C'est pour toutes ces raisons que nous avons contacté le Conseil fédéral et que nous l'avons prié d'examiner s'il n'était pas quand même possible de soumettre au Parlement la solution que nous avions proposée.

3. Télécommunications

3.1. Loi fédérale sur la surveillance du trafic postal et des télécommunications ainsi que sur l'usage de moyens techniques de surveillance

Le Département fédéral de justice et police a mandaté un groupe d'étude pour élaborer une loi fédérale sur la surveillance du trafic postal et des

télécommunications ainsi que sur l'usage de moyens techniques de surveillance. Dans le cadre de la consultation des offices, nous avons eu la possibilité de donner notre avis sur le projet de loi.

Comme nous l'avons déjà expliqué dans notre premier rapport d'activité, la commission de gestion du Conseil national (CdG) a demandé l'adoption de dispositions plus strictes concernant la surveillance du trafic postal et des télécommunications à des fins de poursuite judiciaire. Là-dessus, le chef du Département fédéral de justice et police (DFJP) a mandaté le 15 octobre 1993 un groupe d'étude pour élaborer de telles dispositions. En janvier 1995, les travaux de révision du groupe d'étude relatifs à la surveillance du trafic postal et des télécommunications ont été interrompus. Au début de 1996, le DFJP mandata le même groupe d'étude pour élaborer une loi fédérale sur la surveillance du trafic postal et des télécommunications. Il s'agissait d'y intégrer les travaux préliminaires, d'examiner la création d'un office central pour l'exécution des mesures de surveillance des télécommunications et surtout d'estimer les coûts d'une telle opération. Pour des raisons personnelles et temporelles, nous avons décidé de cesser notre participation dans ce groupe d'étude. Par contre, nous avons eu la possibilité en octobre 1996 de prendre position sur le projet d'une loi fédérale sur la surveillance du trafic postal et des télécommunications ainsi que sur l'usage de moyens techniques de surveillance. Dans le cadre de cette consultation des offices, nous avons pu régler les différends existants ainsi que ceux créés par l'élaboration de la loi.

3.2. TELECOM PTT

Affichage/suppression de l'affichage des numéros d'appel sur les appareils RNIS

Nos demandes dans le domaine de l'affichage des numéros d'appel téléphoniques sur les appareils RNIS ont été en majeure partie bien reçues par Télécom PTT. Mis à part un seul point concernant la taxe unique, nous avons pu nous mettre d'accord.

La fonction offerte par le réseau numérique à intégration de services (RNIS) appelé SwissNet qui consiste à afficher le numéro de téléphone de l'appelant est très pratique et bien utile, puisqu'elle profite à l'appelé en lui indiquant qui l'appelle. Quant à l'appelant, il en bénéficie également, puisque ceci permet par exemple de le rappeler ou de transmettre son appel directement au bon poste interne.
Dans certains cas cependant, l'affichage du numéro de téléphone peut causer de graves atteintes à la personnalité de la personne appelante. Par exemple, un avocat ne désire pas qu'un client qui téléphone depuis son cabinet soit reconnu

Telefonohrbild

comme tel. Si une patiente appelle son employeur depuis le cabinet de son médecin spécialisé, elle risque par cet acte de divulguer des informations très sensibles sur son état de santé. D'autre part, le besoin existe de pouvoir garder secrets les numéros de téléphone réservés pour les appels sortants.
En mars 1996, nous avons envoyé une recommandation (voir p. 115) à Télécom PTT, recommandation dont les principaux points ont été acceptés:
la suppression individuelle du numéro d'appel sera également offerte pour les raccordements analogiques dans le courant de l'année 1998. D'autre part, nos exigences en ce qui concerne l'information de la clientèle sur l'affichage et les possibilités de le bloquer on été remplies. Le seul point sur lequel un accord complet n'a pas pu être réalisé est la gratuité du blocage du numéro d'appel. Télécom PTT a pourtant renoncé à percevoir la taxe mensuelle pour ce service, mais pas à la taxe unique pour la mise en place du blocage.
Nous avons constaté que cette taxe de quinze francs, même si elle semble être basse, peut influencer la décision de l'abonné. Les clients sont forcés de subir des frais pour faire respecter leurs droits, à la suite de développements techniques qu'ils n'ont pas pu influencer. Nous sommes donc d'avis que la taxe de mise en service doit être abolie et avons soumis ce point au Département fédéral des transports, des communications et de l'énergie (DFTCE). Le DFTCE a décidé, en mars 1997, qu'une taxe unique peut être perçue. Le PFPD n'a pas la possibilité de recourir contre cette décision. Par contre, les clients de Télécom PTT, en tant que personnes concernées, peuvent attaquer cette décision devant la Commission fédérale de la protection des données.

- Fonction «forcer l'identification»

Le RNIS prévoit la fonction «forcer l'identification». Un abonné qui dispose de cette fonction est en mesure d'annuler un blocage de l'affichage du numéro bien que celui-ci ait été demandé par la personne appelante. Cette fonction ne doit être disponible que pour un nombre très restreint de services d'urgence (police, pompiers, ambulances) qui sont en mesure de faire valoir des raisons de sécurité évidentes. D'autre part, les abonnés doivent savoir quels sont ces services.
Nous avons eu connaissance de cas dans lesquels d'autres abonnés ont pu utiliser cette fonction. Ceci est inacceptable. Télécom PTT nous a assuré qu'il allait enquêter sur ces cas. Si pour des raisons ne pouvant être immédiatement corrigées, le blocage de l'affichage du numéro de l'appelant ne fonctionne pas de manière fiable, les clients doivent en être informés.

- Appels à l'étranger

Un client de Télécom PTT nous a informé que dans certains cas, bien qu'il ait activé le blocage de l'affichage du numéro d'appel, son numéro a été transmis à l'abonné étranger. Télécom PTT nous a informés qu'il ne pouvait pas garantir que ses partenaires à l'étranger interprètent correctement le signal de blocage. Comme plus haut, il est absolument nécessaire, aussi longtemps que les procédures techniques ne sont pas suffisamment harmonisées sur le plan international, que les clients soient clairement informés de cet état de fait (principe de la transparence).

Annuaires électroniques

Les énormes possibilités de recherche offertes par les annuaires électroniques peuvent mener à la divulgation imprévue et indésirable d'informations relatives aux personnes concernées.

L'annuaire électronique ETV distribué par Télécom PTT, mais également les produits (surtout sous forme de CD-ROM) offerts par d'autres éditeurs privés permettent de faire des recherches très poussées et bien utiles. Celles-ci peuvent parfois mener à des divulgations de données indésirables pour les personnes concernées. Ainsi, il est possible par exemple de trouver tous les abonnés au téléphone habitant une certaine rue, un certain immeuble ou toutes les personnes enregistrées sous un numéro d'abonné (donc les personnes vivant dans un même ménage).
Le fait que des enregistrements anciens restent encore un certain temps dans l'annuaire ETV peut mener à une divulgation délicate et involontaire d'une situation familiale, comme le prouve le cas qu'un client nous a communiqué.
Nous sommes actuellement à la recherche de mesures permettant d'améliorer la protection des données dans ce domaine. Dans ce cadre, nous tiendrons également compte de la suppression de l'obligation actuelle de figurer dans l'annuaire prévue dans la version révisée de la loi sur les télécommunications.

«Fuites» à Télécom PTT

Un communiqué de presse publié en août 1996 a rendu public le fait que des données qui n'étaient pas prévues pour le public ont été diffusées sur un serveur Internet de Télécom PTT qui était lui accessible au public.
Après avoir étudié les documents que Télécom PTT nous a remis suite à notre demande, nous avons pu constater que les données rendues accessibles ne contenaient pas seulement des données à caractère professionnel, mais également quelques données personnelles (listes d'adresses, curriculum vitae).
Cet incident démontre que les mesures de sécurité des données sont encore insuffisantes. Nous sommes d'avis qu'il est absolument nécessaire que les employés soient mieux sensibilisés en ce qui concerne les questions de protection des données. Télécom PTT a engagé des mesures permettant d'améliorer la protection et la sécurité des données.

3.3 LA POSTE

Compte postal

Dans le cadre de l'automatisation du trafic des paiements postaux, les signatures des détenteurs de compte, qui jusqu'ici étaient archivées sur des cartes en papier, ont été numérisées afin de pouvoir les utiliser sous forme électronique (vérification de l'autorisation des personnes participant aux prestations du trafic des paiements). Un détenteur de compte postal y présuma une atteinte à sa personnalité.

Le détenteur de compte postal cité ci-dessus n'était pas d'accord de donner son consentement à ce que sa signature soit numérisée pour être ensuite traitée de

manière électronique. Il fit valoir qu'il considérait ceci comme une atteinte à sa personnalité.
Nos recherches ont démontré que les mesures techniques et organisationnelles prises par la Poste pour éviter un traitement illicite des signatures existantes sous forme électronique étaient adéquates, un abus ne pouvant bien sûr jamais être complètement exclu.
Nous avons également constaté que certaines données traitées peuvent être très sensibles. Les données traitées contiennent, en plus des données d'identification et du solde du compte, aussi les mouvements de compte des 15 derniers mois, les retraits aux Postomat, les achats effectués avec la Postcard etc. Cette quantité de données permettrait sans autre de générer des profils de la personnalité.
C'est pourquoi nous avons examiné si l'accès aux données - nécessaires pour gérer le trafic des paiements postaux - pouvait devenir encore plus restrictif au sein de la Poste et si les autres mesures de sécurité des données étaient suffisantes. Nous avons également examiné les formulaires utilisés pour demander l'ouverture d'un compte postal. La question était de vérifier quelles données sont justifiées par le but de la collecte et si la transparence est assurée pour les clients. Ces recherches sont encore en cours.

3.4. Enregistrement de données concernant des collaborateurs lors de l'utilisation de services Internet

Internet (ou Intranet) devient de plus en plus courant à la place de travail. Il n'est pas étonnant que l'offre abondante peut parfois inciter à des sessions de surf étendues et mal vues par l'employeur. Il n'est pas permis de contrôler le comportement des collaborateurs à cet égard. D'autres contrôles de la part de l'employeur sont cependant clairement limités.

gläserner Mensch

Plusieurs personnes nous ont demandé dans quelles conditions et dans quelle mesure il était permis de traiter des données relatives à l'utilisation de services Internet (ou d'autres services comparables).
En principe, une des tâches d'un supérieur consiste à contrôler que ses instructions soient respectées par ses collaborateurs. Le temps de travail et les ressources de l'entreprise ne doivent pas être utilisées à des fins privées. Un tel contrôle est en règle générale possible sans devoir prendre de mesures techniques détaillées de surveillance.
Un enregistrement complet des activités d'un utilisateur sur Internet et le dépouillement ultérieur des données saisies peuvent cependant aboutir à une grave atteinte à la personnalité des personnes concernées, étant donné qu'il est sans autre possible de générer des profils de la personnalité.
Les services informatiques ne sont donc pas autorisés à analyser l'utilisation que leurs collaborateurs font des services Internet. Ce n'est que dans les cas où des indices concrets font soupçonner la présence d'irrégularités qu'un enregistrement effectué sur ordre de l'organe hiérarchique supérieur peut apparaître adéquat.
Les collaborateurs doivent cependant être préalablement informés quant à l'ampleur des données qui sont enregistrées concernant leur usage d'Internet, comment elles sont traitées et qui les dépouille dans quelles conditions.
Le traitement des données doit être limité à ce qui est absolument nécessaire pour atteindre le but fixé (prévention des abus). Seules les personnes explicitement mandatées à cet effet sont autorisées à consulter les données, et celles qui ne sont plus utilisées doivent être aussitôt détruites.

4. Personnel

Administration fédérale

4.1. Contenu des dossiers du personnel et droit d'accès

L'employeur n'est en droit de conserver des notes et rapports sur le comportement d'un employé dans le dossier du personnel que dans la mesure où ceux-ci sont importants pour les rapports de travail. Les qualifications et les appréciations font partie des données les plus importantes d'un dossier du personnel et ne peuvent en être retirées que lorsqu'elles ne sont plus nécessaires à l'exécution du contrat de travail. L'employé dispose en principe d'un droit d'accès illimité.

La question de savoir ce qui pouvait légitimement être contenu dans un dossier du personnel a été posée par un employé des PTT, après que celui-ci a trouvé des comptes-rendus concernant son comportement dans son dossier du personnel. Ceux-ci concernaient principalement des dommages causés à de petits objets dans l'entreprise. Ces comptes-rendus ont finalement cessé, étant donné qu'ils ne donnaient pas lieu à des mesures disciplinaires.
Nous avons rendu attentif les PTT au fait que les documents et les rapports concernant des événements particuliers ayant eu lieu dans l'entreprise ne peuvent être versés au dossier du personnel que s'ils sont de manière objective vraiment nécessaires aux rapports de travail. Des documents du genre mentionné ci-dessus ne peuvent donc pas être légitimement conservés dans le dossier du personnel. Au cas où des documents sans importance se trouvent dans le dossier du personnel, ils

doivent en être retirés à l'occasion d'un triage régulier. Ceci vaut également pour les documents qui ne perdent leur importance pour l'exécution du contrat de travail qu'après un certain temps. D'autre part, les informations doivent être conservées dans le dossier du personnel aussi longtemps qu'elles sont effectivement nécessaires. Le fait de retirer prématurément et définitivement des formules de qualification du dossier du personnel au cours d'une procédure de demande de renseignements peut être considéré comme une durée de conservation excessivement courte. Cette violation du principe de proportionnalité peut dans certaines circonstances représenter en plus une non-observation du principe de la bonne foi.
Au début, le droit d'accès de l'employé des PTT a été à plusieurs reprises refusé. Ce n'est qu'après intervention de la direction d'arrondissement postal qu'on lui accorda le droit de consulter son dossier. La possibilité de photocopier le contenu du dossier n'a été offerte que plus tard. Nous avons rendu attentif les PTT au fait que toute personne était en droit de demander au maître de fichier si des données la concernant étaient traitées.
Nous avons en outre retenu que le maître du fichier est tenu de fournir des renseignements complets et conformes à la vérité sur le contenu du dossier du personnel. La consultation du dossier par la personne concernée sur place n'exclut pas pour autant la possibilité d'en photocopier le contenu. Le maître du fichier ne peut refuser, restreindre ou différer la communication des renseignements demandés que si une loi au sens formel le prévoit ou que l'intérêt prépondérant d'un tiers l'exige. Un organe fédéral peut en outre refuser, restreindre ou différer la communication des renseignements dans la mesure où un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Confédération l'exige, ou si la communication des renseignements risque de compromettre une instruction pénale ou une autre procédure d'instruction. L'employeur est en outre tenu d'informer les employés de leur droit d'accès. Nous avons ensuite souligné la signification de l'article 328 *b* du Code des obligations (CO). Cette disposition fait office de droit administratif supplétif et est applicable par analogie aux traitements de données effectués par la Confédération. Elle stipule que le maître de fichier n'est en droit de traiter que les données dont il a objectivement vraiment besoin pour atteindre un but donné. Le service du personnel de la direction d'arrondissement postal concernée a accepté de gérer ses dossiers du personnel en accord avec les principes de protection des données et d'informer les employés sur leur droit d'accès, le cas échéant dans la lettre d'engagement.

4.2. Vidéosurveillance à la place de travail

L'utilisation de systèmes de surveillance et de contrôle qui surveillent le comportement des employés à leur place de travail n'est pas autorisée. Si de tels systèmes deviennent nécessaires pour d'autres raisons, ceux-ci doivent être conçus et installés de manière à ne pas entraver la santé, la personnalité et la liberté de mouvement des employés.

Un employé des PTT s'est informé auprès de nous sur la légitimité d'une vidéosurveillance à la place de travail. Nous lui avons communiqué que les employés ont droit à un degré de vie privée approprié à leur place de travail. Ils doivent être informés des méthodes de surveillance mises en oeuvre. Une surveillance électronique permanente n'est pas autorisée. Les supérieurs qui violeraient ces

principes doivent s'attendre à ce que des mesures disciplinaires soient prises à leur encontre ou qu'ils soient licenciés (voir les directives de l'Organisation internationale du travail OIT). En ce qui concerne les systèmes de surveillance utilisés pour des raisons de sécurité (par ex. pour surveiller le processus de fabrication), il y a lieu de veiller à ce que le procédé choisi ménage la personnalité des employés. Ceci vaut également pour les installations utilisées pour la gestion de la production. Nous avons donc proposé aux PTT de réglementer la surveillance à la place de travail dans des directives internes.

4.3. Surveillance du téléphone à la place de travail

Dans certaines conditions, un central téléphonique peut représenter un système de surveillance et de contrôle. Ceci est le cas par exemple lorsque les numéros de téléphone de tous les appels entrant et sortants sont affichés et enregistrés, ou que la durée ou le coût des communications individuelles est enregistré. Font également et surtout partie de cette catégorie les systèmes téléphoniques permettant d'écouter les conversations sans que les personnes concernées en soient conscientes. Il n'est cependant pas permis de contrôler le comportement des employés en utilisant de tels systèmes de surveillance et de contrôle. Leur utilisation n'est admissible que pour des raisons de sécurité ou pour la gestion de la production (voir notre 2ème rapport d'activité, p. 138 ss).

Fax

Un représentant d'une entreprise privée s'est renseigné auprès de nous sur l'admissibilité de l'utilisation de centraux téléphoniques à des fins de surveillance. Nous lui avons répondu que les employeurs ne peuvent utiliser des centraux téléphoniques à de telles fins que si les employés concernés en ont été informés au préalable. L'enregistrement des numéros de téléphone appelés pour des raisons professionnelles est permis, pour autant qu'il ne serve pas à surveiller le comportement de l'employé (mais plutôt par ex. pour permettre la facturation de ces communications aux clients). Les numéros de téléphone appelés par les employés pour des raisons privées ne doivent en aucun cas être enregistrés sous une forme identifiable, à moins que les communications téléphoniques privées n'aient été interdites de manière générale. Cet enregistrement devrait uniquement servir aux personnes concernées (par ex. pour vérifier le montant des communications privées déduites de leur salaire). Dans le cas où des irrégularités évidentes apparaîtrait dans les coûts des communications pour certains postes, le chef du personnel (par ex.) peut demander - après en avoir informé le personnel - un relevé détaillé pour le poste en question. Ce relevé doit présenter les numéros des raccordements privés qui ont été appelés sous une forme non identifiable. Un soupçon d'irrégularités peut être admis si les coûts de communications téléphoniques d'un poste représentent plus du double de la moyenne de l'unité d'organisation concernée au sein de l'entreprise, sans que cela puisse être expliqué par des raisons propres à l'entreprise. Le contenu des communications téléphoniques ne peut être enregistré qu'à des fins de contrôle des performances (par ex. lors de ventes par téléphone ou lors de cours de formation) ou pour des motifs de sécurité. Cette mesure de contrôle très incisive n'est admissible que si la personne dont la communication est enregistrée ou écoutée y a donné son accord et pour autant qu'elle en soit chaque fois informée à temps et de manière claire (par ex. par un signal optique ou acoustique).

4.4. Le projet BV-PLUS

Le système BV-PLUS prévoit le traitement de données sensibles (voir p. 138 ss du 1er rapport d'activités et p. 141 du 3ème rapport d'activités). C'est pourquoi nous avions demandé à l'Office fédéral du personnel de créer une base légale pour ce système dans une loi au sens formel. Nous avons également demandé que le système BV-PLUS ne soit utilisé de manière centralisée que pour la gestion des salaires. Finalement, nous avons émis une recommandation qui fut déférée au Département fédéral des finances.

C'est au début de 1996 que nous avons appris que le système central de traitement de données de l'Administration fédérale BV-PLUS allait prochainement être mis en service. Nous avions déjà rendu attentif précédemment l'Office fédéral du personnel (OFPER) à la tendance au traitement décentralisé des données dans l'Administration fédérale (voir notre 1er rapport d'activités, p. 138 ss). Nous avions salué cette tendance à la décentralisation pour des raisons relevant de la protection des données, mais aussi pour des raisons de rentabilité et d'efficacité. Nous avions exigé que cette dernière soit retenue dans un projet d'ordonnance sur la protection des données des fonctionnaires fédéraux. Le système ne devait être utilisé de manière centralisée que pour la gestion des salaires.
A cause du traitement prévu de données sensibles par le système BV-PLUS, nous avions insisté sur la nécessité de créer une base légale au sens formel pour ce système. L'OFPER a cependant rejeté cette exigence. Cet office était d'avis que des

exigences réduites envers la base légale existaient, étant donné que BV-PLUS ne traitait pas de données sensibles ni de profils de la personnalité. Dans le cadre de la décentralisation des traitements de données dans l'Administration fédérale, le système BV-PLUS - selon l'avis de l'OFPER - ne se distingue pas du système d'information du personnel existant PERIBU.
Nous avons recommandé à l'OFPER d'utiliser BV-PLUS uniquement pour la gestion des salaires et seulement après création des bases formelles et matérielles. L'OFPER a rejeté notre recommandation. Nous avons alors soumis la question pour décision au Département fédéral des finances. Celui-ci nous a fait savoir qu'une base juridique de niveau réglementaire serait créée pour BV-PLUS.
Le Département des finances nous a en outre informés que BV-PLUS ne serait plus mis en oeuvre avec le logiciel prévu à l'origine, mais avec le logiciel standard SAP R3 HR.
Nous avons également rendu attentif le Département des finances au fait qu'il était nécessaire de créer une base légale au sens formel pour le système de gestion du personnel de l'Administration fédérale.
A notre avis une loi au sens formel est nécessaire dans ce cas, non seulement parce que le traitement concerne des données sensibles, mais également parce que la législation sur les fonctionnaires en vigueur aujourd'hui ne prévoit pas la compétence de l'OFPER pour le traitement de ces données. Accessoirement, la création d'une telle base légale permettrait de régler la répartition des tâches entre l'OFPER et les différents services du personnel.

4.5. INSIGHTS - Système d'évaluation du personnel

Depuis quelques années, la version «management-collaborateurs» de ce produit est à disposition des unités administratives de la Confédération sur disquettes. Outre les éléments soulignés dans notre deuxième rapport d'activités (p. 142 ss), nous avons conseillé de ne pas utiliser ce type de test à des fins de recrutement, mais de le considérer comme un instrument possible de gestion d'une équipe. La plupart des disquettes n'étant pas protégées par un mot de passe, nous avons également souligné la nécessité d'anonymiser les analyses dès le début. Vu la durée de validité limitée des résultats, nous avons finalement déconseillé le stockage et la conservation systématiques des analyses (Cf. également Annexe p. 211 du présent rapport)

Ce n'est pas un software qui est vendu, mais un certain nombre d'analyses qui, au sein de l'administration fédérale, est mis à disposition sur disquettes.
Il est recommandé par le vendeur de respecter certains principes d'utilisation, à savoir notamment le caractère facultatif du test, le fait que ce dernier appartient à la personne concernée et qu'après deux ans, les résultats de l'analyse sont obsolètes. Ces recommandations ne font cependant pas partie intégrante du contrat, et aucun code éthique n'est imposé aux acheteurs des tests, autorisés à acquérir des analyses et à les utiliser sans formation préalable.
Il est possible de protéger la disquette par deux mots de passe distincts, l'un permettant l'introduction des données pour analyse et l'autre rendant possible l'impression des résultats. On nous a également assuré que le niveau de sécurité est élevé (autodestruction du programme en cas de tentative de modification des données et piratage impossible).
Une fois introduites, les données ne sont plus modifiables, à l'exception des données relatives à l'identité qui peuvent être changées une seule fois.

Les collaborateurs du préposé qui se sont soumis au test ont évalué les résultats, respectivement les ont fait évaluer par une personne les connaissant bien. Le taux d'exactitude des résultats a été apprécié en moyenne entre 70 et 80%.
Nous avons tout d'abord souligné que, dans le cas où, comme dans notre Secrétariat, une disquette non protégée par un mot de passe est mise en circulation, il est impératif d'anonymiser les analyses dès le début, la clé d'identification n'étant connue que de la personne concernée.
Si ce produit est utilisé systématiquement comme instrument de gestion du personnel, les disquettes sont protégées au moins par un mot de passe (deux si l'on souhaite séparer les tâches d'introduction et d'impression). Au maximum deux personnes du service du personnel sont autorisées à accéder aux données, une anonymisation étant également envisageable dès que le traitement des analyses le permet.
Nous avons au demeurant déconseillé le stockage et la conservation systématiques des analyses, vu la durée de validité limitée des résultats.
En raison du caractère général de l'analyse, nous avons en outre souligné que ce produit ne peut pas être utilisé à des fins de recrutement de personnel, mais plutôt comme instrument de gestion d'une équipe.
Il est finalement impératif que ce type de tests soit utilisé conformément aux Directives de l'Office fédéral du personnel sur l'application de méthodes de test individuelles et collectives (cf. Annexe p. 211 du présent rapport).

4.6. Demandes de références contre le gré de la personne concernée

Dans le cadre d'un poste mis au concours dans l'Administration fédérale, des renseignements ont été recueillis auprès de tiers. Du point de vue de la protection des données, il n'est en principe pas permis de demander des références sans l'assentiment préalable du candidat au poste.

Un employé de l'Administration fédérale s'est plaint auprès de nous, qu'à l'occasion de sa candidature auprès de l'Administration fédérale, des références ont été demandées auprès de tiers sans son accord. Les tiers en question n'avaient pas été mentionnés comme références dans la lettre de candidature. A ce propos, nous lui avons communiqué les principes suivants: les conditions des traitements de données lors d'une candidature ne sont régies ni par la législation sur les fonctionnaires, ni par la loi sur la protection des données ou l'ordonnance d'exécution qui s'y rapporte. L'admissibilité par principe de traitements de données en rapport avec des candidatures d'emploi découle cependant des tâches générales des départements de l'Administration fédérale.
La seule indication se rapportant à l'ampleur des traitements de données admissibles dans le cadre d'une candidature au sein de l'Administration fédérale peut être trouvée dans la circulaire de l'Office fédéral du personnel (OFPER) sur le traitement de données personnelles dans l'Administration fédérale du 26 janvier 1984. Ce document est toujours en vigueur aujourd'hui, malgré le fait que les directives sur lesquelles il se fonde ont été abrogées. Le chiffre 2.4.1. de cette circulaire dit: «Si les documents fournis par le candidat à l'emploi ainsi que les références indiquées ne sont pas suffisants pour l'appréciation, la démarche à suivre doit être discutée avec le candidat». Il découle de ceci que des références supplémentaires ne peuvent être demandées qu'avec l'assentiment de la personne concernée. En outre, nous tenons à relever que nous optons également pour cette solution dans notre «Guide pour le

traitement de données personnelles dans le domaine du travail par des personnes privées (p. 8 et 9)». Les principes qui y sont mentionnés concernent le traitement de données dans le domaine privé, mais sont également applicables par analogie à l'Administration fédérale.

5. Assurances

Assurances sociales

5.1. Assurance-invalidité et protection des données

Des questions relatives à la «cohabitation» entre la législation sur l'assurance-invalidité (AI) et la protection des données nous ont été posées par l'Office fédéral des assurances sociales (OFAS). En voici une sélection, portant avant tout sur la problématique de la communication de données à des tiers, ainsi que les éléments de réponse que nous y avons apportés au cours de l'exercice écoulé.

En matière d'assurance-invalidité (AI), la problématique des relations entre cette législation et celle de la protection des données se pose avec acuité, à l'instar des autres secteurs des assurances sociales. Voici un morceau choisi de questions au sujet desquelles nous avons été appelés à nous prononcer:

- peut-on se fonder sur l'article 19, 1er alinéa, lettre d, LPD, pour communiquer des données, même sensibles, à des tiers?

En principe, des données personnelles, même sensibles, peuvent être communiquées dans une certaine mesure à des tiers. Cependant, en matière d'AI, il faut tenir compte de l'article 19, 4e alinéa, lettre b, LPD qui réserve «une obligation légale de garder le secret». L'article 50, 1er alinéa, de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS), applicable également à l'AI, prévoit une telle obligation. Les exceptions prévues par le Conseil fédéral sont réservées. Elles sont ancrées à l'article 209bis du règlement sur l'assurance-vieillesse et survivants (RAVS). C'est donc sur cette disposition, et non sur l'article 19 LPD, que les organes AI doivent se fonder lorsqu'ils envisagent de communiquer des données.

- l'Office fédéral des assurances sociales (OFAS) peut-il se baser sur l'article 19, 2e alinéa, LPD, pour indiquer à un tiers si une personne déterminée est ou non annoncée à l'AI?

Nous avons ici répondu par la négative. Certes, un organe fédéral peut (mais ne doit pas) communiquer sur demande les nom, prénom, adresse et date de naissance d'une personne. Encore faut-il que ces informations ne permettent pas de déduire d'autres indications sur l'intéressé, en particulier des données sensibles.
Or, ce serait le cas si la division AI de l'OFAS communiquait l'identité d'un intéressé, car cela indiquerait également que celui-ci est annoncé à l'AI.

- est-il vrai que si la personne concernée s'y oppose au sens de l'article 20 LPD, toute communication de données à son sujet doit être refusée par l'OFAS?

Effectivement, si une personne s'oppose à la communication de données la concernant, sa volonté doit être respectée même si la communication envisagée serait en soi licite.
Encore faut-il que cette opposition ne puisse pas être levée par un des motifs énunérés à l'article 20, 2e alinéa, LPD. Cet alinéa prévoit qu'une opposition peut être levée ou rejetée si l'organe fédéral est juridiquement tenu de communiquer les données ou si l'accomplissement de ses tâches risque d'être compromis par le défaut de communication.
Finalement, pour être valable, une demande de blocage doit porter sur des données précises et se fonder sur un intérêt légitime actuel rendu vraisemblable par la personne concernée.

- l'OFAS peut-il se baser sur l'article 22 LPD pour légitimer une communication de données à des fins de recherche sans le consentement de la personne concernée?

Nous avons rappelé que l'article 22 LPD n'est pas applicable, en raison de l'obligation légale de garder le secret réservée à l'article 19, 4e alinéa, LPD.
En matière d'AI, selon l'article 50 LAVS, respectivement l'article 209bis RAVS, deux voies sont possibles pour permettre la communication de données à des tiers: l'autorisation de l'OFAS ou l'autorisation écrite de la personne concernée.
L'OFAS peut donc renoncer à requérir le consentement de l'intéressé en autorisant une communication de données, par exemple sous forme de consultation des dossiers AI. Cet office sera alors tenu de délivrer son autorisation sous forme de décision dont les personnes concernées devront être informées, afin de leur permettre le cas échéant d'interjeter recours (article 209bis, 3e alinéa, RAVS).

Nous avons finalement rappelé que l'OFAS est responsable au premier chef du respect des principes ancrés dans la LPD. Il est dès lors important qu'il veille, notamment en matière de communication de données, à ce que des règles uniformes soient appliquées par les organes soumis à sa surveillance, tels les offices AI.

5.2. Communication systématique du diagnostic aux assurances-maladie

Ce que nous avons exposé sous le titre «5.1. Communication systématique du diagnostic aux assurances-maladie» (voir notre 3ème rapport d'activités p. 146 ss) pour interpréter les alinéas 3 et 4 de l'article 42 LAMal est, de notre point de vue, toujours valable. Malheureusement cela a été partiellement la source de malentendus que nous aimerions éclaircir ici. Il ressort du texte de la loi que des diagnostics exacts ne doivent être communiqués que sur demande, donc pas de manière systématique (c.-à-d. pas dans tous les cas). Il y a lieu de communiquer à l'assureur les «données dont il a besoin pour vérifier le calcul de la rémunération et le caractère économique de la prestation» (article 42, 4e alinéa, LAMal). Quelles sont ces données au regard du principe de proportionnalité? Il ne s'agit que des informations permettant cette vérification (critère de l'aptitude) et parmi celles-ci uniquement les informations qui sont absolument indispensables (critère de la nécessité).

5.3. Renonciation à délier du secret médical pour la taxe militaire

L'Office fédéral des affaires sanitaires de l'armée ainsi que l'Office fédéral de l'assurance militaire doivent communiquer régulièrement des données relatives à la santé aux autorités cantonales chargées de percevoir la taxe militaire. Pour des raisons d'économie administrative, il est prévu pour les premiers examens de renoncer à l'avenir à obtenir le consentement des personnes concernées.

Dans la loi fédérale sur la taxe d'exemption du service militaire, une disposition explicite réglant la communication de données sensibles relatives à la santé fait défaut. Se pose donc la question de savoir si une communication de ces données sensibles sans le consentement des personnes concernées ne viole pas le secret médical conformément au code pénal ou la loi sur la protection des données. Dans un avis de droit sur la première question, l'Office fédéral de la justice a estimé qu'en tenant compte des circonstances spéciales on ne pouvait pas retenir une violation du secret médical au sens du code pénal.
Si l'on présume le *consentement tacite* des personnes concernées lors de la communication de données *non* sensibles, la communication de telles données *dans des cas isolés* serait admissible selon la loi sur la protection des données. Avec la mise en réseau croissante des données, on peut cependant douter que les personnes concernées (même si elles attendent une décision de l'autorité en leur faveur) soient prêtes à accepter tous les traitements de données, alors que des traitements moins étendus suffiraient à leur avis. Dans le cas cependant où les communications concernent également des *données sensibles sur la santé*, *on ne peut plus à notre avis présumer un consentement tacite*. La lacune dans le texte législatif concernant la taxe d'exemption militaire devrait être comblée d'ici le 1er juillet 1998 (voir aussi p. 103).
Nous avons donné notre accord, limité jusqu'au 1er juillet 1998, à la pratique prévue. Nos recherches ont en effet montré que le nombre de données communiquées lors d'un premier examen était minime.

Assurances privées

5.4. Feuilles d'information et clauses de consentement

La conception des feuilles d'information et des clauses de consentement dans le domaine des assurances privées semble s'imposer dans la pratique et a été poursuivie en collaboration avec les assurances. Relevons tout d'abord une amélioration considérable de la transparence des feuilles d'information et des clauses de consentement. D'autre part, pour la première fois, une compagnie d'assurances s'est déclarée prête à requérir le consentement des assurés (ce que nous avions demandé) pour chaque circonstance spécifique (demande d'affiliation, devoir d'annonce, accident, prestation, sinistre, etc).

Il convient tout d'abord de se reporter- notamment pour ce qui est des clauses de consentement - aux explications détaillées figurant dans le troisième rapport d'activités (p. 148 ss).
Le but de la feuille d'information relative à la protection des données est d'informer l'assuré de manière aussi complète que possible du traitement de données le concernant (principe de transparence). Il doit pouvoir reconnaître qui communique quelles données à qui et dans quel but. Du reste, les compagnies d'assurance

(personnes morales) ne sont dispensées d'annoncer bon nombre de fichiers au PFPD que si les intéressés ont connaissance du traitement de leurs données personnelles.
Le contenu des feuilles d'information que nous avons examinées est plus précis et plus complet qu'auparavant. En particulier, le client est informé en détail de ce qu'il peut demander (données disponibles, but, catégories de données personnelles traitées, participants au fichier, destinataires des informations). Dans la pratique, il faut accorder l'attention nécessaire au droit d'accès. C'est en effet l'élément fondamental du droit de la protection des données.
Les clauses de consentement que nous avions présentées ont été également adoptées par des assurances. Le but du traitement des données ainsi que les personnes ou services avec lesquels l'assurance échange des données sont mentionnés de manière plus claire et exhaustive.
Au surplus, nous n'avons jamais cessé de demander que la personne concernée puisse révoquer en tout temps une clause de consentement. Cette possibilité de révocation permanente doit donc figurer dans toute clause de consentement.
Par ailleurs, l'assurance doit toujours requérir le consentement de l'assuré dans le contexte d'un événement spécifique. Nous sommes en contact avec une compagnie qui a élaboré des clauses de consentement pour chaque secteur d'assurance et chaque circonstance selon un système de modules. Nous allons illustrer cette méthode à l'aide d'un exemple, celui de l'assurance-maladie collective : lors de la demande d'affiliation ou de l'annonce d'un cas de maladie, on demande - selon la situation - les consentements spécifiques à la personne concernée. En outre, nous tenons à ce que sur les formulaires d'assurances, les clauses de consentement figurent en caractères gras à proximité immédiate de la signature.
Enfin, au stade initial d'un contrat d'assurance, il convient de demander le consentement de la personne à assurer en vue de l'utilisation de ses données personnelles à des fins de marketing. Là aussi, le droit permanent de révocation sera souligné ainsi que le fait qu'un blocage des données à des fins de marketing ne doit avoir aucune répercussion négative sur la conclusion du contrat. En effet, la conclusion du contrat ne doit pas dépendre du fait que quelqu'un donne ou non son consentement.

5.5. Défaut de confidentialité des données médicales figurant sur les formulaires d'assurance

Un employeur a eu involontairement connaissance - dans le cadre d'une déclaration pour une assurance collective d'indemnités journalières - de données concernant la santé d'une salariée. Du point de vue de la protection des données, ce cas constitue une violation de la personnalité de la salariée dans la mesure où il n'existe pas de motifs justificatifs.

Nouvellement engagée, une salariée avait l'intention de s'assurer auprès de l'assurance collective d'indemnités journalières de son nouvel employeur. Elle décida néanmoins de ne pas remplir intégralement le questionnaire médical figurant sur le formulaire d'inscription. Le preneur d'assurance, et de ce fait le partenaire contractuel de l'assurance, n'était toutefois par la salariée à assurer, mais une fondation créée à cet effet, dont l'adresse était identique à celle de l'employeur. L'assurance retourna le formulaire lacunaire à la fondation, donc à l'employeur, pour complément d'information en priant de bien vouloir faire remplir intégralement le

formulaire en question. La salariée comme l'employeur se plaignirent auprès de l'assurance en invoquant une incompatibilité avec la protection des données.
Nous avons aussi estimé que du point de vue du droit de la protection des données, la communication à des tiers de données sensibles telles les données sur l'état de santé n'était pas autorisée. Dans le cas présent, on peut vraiment se demander si la fondation (et du même coup l'employeur) doit avoir accès aux données concernant la santé de la salariée. En théorie, on pourrait imaginer que l'employeur dénonce le rapport de travail parce que la salariée souffre d'une maladie précise. Dans tous les cas, il est absolument inutile qu'à l'exception de la personne à assurer, un tiers ait accès aux données médicales de celle-ci. En effet, elle est la seule à pouvoir garantir l'exactitude des données concernant sa santé. Le formulaire médical a donc été envoyé à l'employeur de manière contraire à la loi, de plus sans motifs justificatifs.
La compagnie d'assurance compétente s'est en définitive rangée à notre avis, selon lequel les données concernant la santé ne doivent pas être communiquées à l'employeur. Par ailleurs, elle a remanié les formulaires d'inscription dans notre sens.

5.6. Regroupement automatique de divers dossiers d'assurance dans le cadre de la conclusion d'un contrat d'assurance

Une avocate avait l'intention de conclure une assurance-responsabilité professionnelle auprès d'une compagnie d'assurances. L'agent d'assurances entendait intégrer à cette occasion deux dossiers la concernant - dont l'un portait sur un accident de voiture survenu en 1986 - au nouveau dossier. Toutefois, le regroupement automatique de tous les dossiers antérieurs au moment de la conclusion d'un nouveau contrat d'assurance peut aisément conduire à une violation de la loi sur la protection des données.

Une compagnie d'assurances désirait informer une avocate installée à son compte depuis peu des possibilités offertes par l'assurance-responsabilité professionnelle. Lors de la première entrevue, l'agent d'assurances lui présenta deux listings qui se rapportaient à deux dossiers précédents. L'un concernait un accident de voiture survenu en 1986, au cours duquel l'assurance avait agi à l'encontre de l'avocate comme assureur du conducteur fautif. L'autre dossier par contre portait sur l'assurance-responsabilité professionnelle de son ancien employeur, auprès duquel elle avait fait son stage d'avocat. L'avocate fut en outre informée incidemment que le montant assuré de son ancien employeur s'élevait «seulement» à un million de francs. L'agent d'assurances avait finalement l'intention de joindre les deux dossiers en question au nouveau dossier concernant l'assurance-responsabilité professionnelle.
Le regroupement automatique de différents dossiers est rapidement susceptible de mener à une violation des principes de la protection des données. Par exemple joindre le «dossier de l'accident de voiture» au nouveau «dossier responsabilité professionnelle» va à l'encontre du principe de la proportionnalité. En effet, la conclusion d'un contrat d'assurance-responsabilité professionnelle ne nécessite pas que les données requises dans ce dernier contrat soient mises en relation avec les données - surtout les données personnelles - relatives à un accident d'automobile remontant à dix ans. Par ailleurs, il est également contraire à la loi de communiquer le montant assuré de l'ancien employeur - sans son autorisation - à des tiers, même à une ancienne employée. En tout état de cause, si des personnes extérieures à

l'entreprise, par exemple des clients, l'apprenaient, il pourrait y avoir préjudice commercial.
En outre, nous avons demandé que la personne à assurer soit informée au préalable et en détail du contenu du traitement des données. Il conviendra en dernier lieu de requérir le consentement, rédigé de la manière la plus claire possible, de la personne à assurer pour pouvoir intégrer des dossiers internes aux documents établis en vue d'un nouveau contrat (voir aussi p. 153 Feuilles d'information et clauses de consentement).

5.7. Système central d'information ZIS

Le ZIS est un fichier du secteur des assurances sur les procédures pénales et civiles pendantes ou closes. Son objectif principal est de protéger les compagnies d'assurance des manoeuvres frauduleuses.

Le fichier ZIS a été annoncé au PFPD. Etant donné qu'il renferme des données sensibles et qu'une personne privée a attiré notre attention à ce sujet, nous avons examiné surtout sa légitimité.
Les compagnies d'assurance annoncent au secrétariat du ZIS les preneurs d'assurance, les assurés, les lésés, les conducteurs, les personnes ayant annoncé un cas d'assurance, leurs auxiliaires et autres participants en relation directe ou indirecte avec un contrat d'assurance ou un cas d'assurance lié à un délit. Entrent notamment en ligne de compte les éléments constitutifs suivants: abus de confiance, recel, escroquerie, gestion déloyale ainsi que faux et usage de faux. Outre les délits accomplis, la tentative, l'incitation ainsi que la complicité sont également enregistrées. Dès qu'une compagnie d'assurance a connaissance de procédures d'enquête policière ou judiciaire et qu'il y a soupçon, elle l'annonce immédiatement au secrétariat. Les modifications ou l'issue d'une procédure pénale ou civile sont aussi immédiatement transmises au secrétariat. Les données ne sont pas traitées par informatique, mais saisies sur papier. Le secrétariat transmet les données régulièrement mises à jour aux compagnies d'assurance.
Les données concernant des procédures civiles ou pénales pendantes ou closes sont des données sensibles. Leur traitement et en particulier leur communication à d'autres sociétés (tiers) nécessitent un motif justificatif. Le but du ZIS est d'identifier les prétentions d'assurances malhonnêtes et d'empêcher la conclusion de contrats d'assurance dans un contexte frauduleux. Cela devrait permettre d'alléger les primes dans l'intérêt des assurés. Dans ce contexte, il convient de peser les intérêts en jeu entre le traitement de données sensibles et les intérêts privés prépondérants de la compagnie ou des intérêts publics prépondérants.
On ne peut pas, dans le cas présent, invoquer le motif justificatif du traitement de données personnelles concernant un cocontractant, en relation directe avec la conclusion ou l'exécution d'un contrat, car la communication à d'autres sociétés par le ZIS ne se situe pas dans le cadre d'une telle relation. Il convient donc d'écarter la présence d'un intérêt privé prépondérant.
La situation économique actuelle semble avoir une influence à la hausse sur les cas d'escroquerie à l'assurance, ce que confirme le nombre de cas annoncés au ZIS (79 en 1992, 466 en 1996). Vu sous cet angle, l'assuré honnête a un intérêt légitime à ce que les assurances n'aient pas à payer des montants indûs qui se traduiraient par une augmentation des primes. Nous sommes ici parvenus à la conclusion qu'un

intérêt public prépondérant de l'ensemble des assurés justifie le traitement de ces données personnelles.
Par ailleurs, nous avons constaté que le traitement de données personnelles repose sur un réglement dont l'application est contrôlée par un organe de surveillance indépendant. La communication mensuelle des dernières modifications (jugements) sur papier garantit en outre l'exactitude et l'actualité des données. Ces mesures permettent d'empêcher que l'utilisation abusive de données sensibles se répande sans frein (par ex. échange incontrôlé entre les compagnies d'assurances). Chaque compagnie a la responsabilité d'estimer et de décider s'il faut ou non annoncer un cas.

6. SANTE

6.1. Contrôle de l'assurance-maladie obligatoire en vertu de la LAMal

Selon la nouvelle loi sur l'assurance-maladie, les cantons sont responsables du respect de l'obligation de s'assurer. Mais un canton qui, à cet effet, demande aux assurés une copie du certificat d'assurance contrevient aux dispositions générales sur la protection des données. Il en va de même lorsque les caisses-maladie envoient par informatique aux cantons les renseignements d'assurance requis.

Contrôle au moyen du certificat d'assurance

On nous a demandé à plusieurs reprises si les cantons étaient réellement autorisés à demander une copie du certificat d'assurance pour contrôler le respect de l'obligation de s'assurer. La question de savoir dans quelle mesure ce procédé est conforme à la protection des données relève fondamentalement de la compétence des autorités cantonales chargées de la protection des données. Cela ne doit néanmoins pas nous empêcher de prendre position.
En vertu de la nouvelle LAMal, les cantons sont chargés de veiller au respect de l'obligation de s'assurer. Les cantons et les communes sont libres de s'y prendre concrètement comme ils le veulent. Certaines communes par exemple demandent une copie du certificat d'assurance, lequel contient en général outre les données relatives à l'assurance obligatoire, des renseignements sur les assurances complémentaires, les réserves, etc. Ce qui est disportionné et constitue de ce fait une atteinte aux principes généraux de la protection des données.
A notre avis, il suffit que les cantons (ou les communes) informent en détail leurs habitants par une feuille d'information sur l'obligation de s'assurer. Ils peuvent indiquer en plus sur cette feuille que les personnes qui ne remplissent pas leur obligation de s'assurer seront affectées d'office par les autorités cantonales à un assureur. Enfin, ils peuvent signaler les suites pénales éventuelles en cas de contravention. Une autre solution serait aussi que les cantons demandent une confirmation écrite aux assurés.

Contrôle de la communication de données des caisses-maladie

Nous avons été consultés par une entreprise privée qui propose aux autorités cantonales des prestations informatiques permettant le contrôle de l'obligation de

s'assurer conformément à la LAMal. Selon le concept qui nous a été soumis, les caisses-maladie devraient à cet effet fournir aux autorités cantonales des données sur leurs assurés domiciliés dans le canton. Dans la question qui nous a été posée, il était entre autres mentionné qu'un canton avait déjà conclu un contrat de prestations de services. Pour ce canton, il y avait eu «soumission contractuelle à la protection des données». L'entreprise envisageait d'offrir cette prestation au niveau national.
Les caisses-maladie agissant dans le cadre de cette obligation comme organes de la Confédération, ont besoin d'une base légale pour toute communication de données personnelles. Les seules exceptions à cette règle concernent des cas particuliers de communications de données. On ne trouve de *base légale* ni dans la LAMal, ni dans l'ordonnance sur la LAMal, donc la communication de données est ici illicite.
Le manque de *proportionnalité* du traitement des données constitue un autre problème. Avant cette obligation de s'assurer, plus de 99 % de la population était déjà assurée. Il ne semble donc *pas approprié* de communiquer une si grande quantité de données concernant l'ensemble de la population afin qu'une très petite partie de celle-ci se plie à cette obligation. Par conséquent, une communication, qu'elle soit unique ou périodique, aux autorités cantonales n'est donc pas appropriée pour contrôler effectivement cette obligation. En effet, ces communications ont toujours lieu à une date de référence, après laquelle de nouveaux habitants peuvent arriver dans le territoire contrôlé ou d'anciens habitants peuvent partir. Le PFPD a été déjà consulté dans des cas où des personnes avaient reçu des mises en demeure du contrôle de l'habitant alors qu'elles avaient déjà déménagé.
Un contrôle approprié de cette obligation de s'assurer ne concerne qu'une seule fois l'ensemble de la population du canton et se limite par la suite à la vérification des mouvements de population, qui peuvent être effectués directement par le contrôle de l'habitant. Dans un premier temps, on peut attirer l'attention des habitants du canton à une date fixe - ainsi que nous l'avons déjà mentionné - par une feuille d'information faisant état de leur obligation de s'assurer et des conséquences pénales en cas de non observation. On peut également envisager de demander aux assurés de confirmer par écrit qu'ils sont véritablement assurés. Après établissement de la situation à la date de référence, il suffit ensuite de demander une attestation d'assurance aux nouveaux arrivants seulement. La LAMal requiert en effet qu'une personne qui est une fois assurée le reste pour toujours. En effet, en vertu de l'article 7, 5e alinéa, LAMal, l'affiliation auprès de l'ancien assureur cesse seulement lorsque le nouvel assureur lui a communiqué «qu'il assure l'intéressé sans interruption de la protection d'assurance».
Ce contrôle de l'obligation de s'assurer répond au principe de proportionnalité. De plus, il nécessite moins de démarches et par conséquent engendre un moindre coût.

6.2. Statistiques médicales des hôpitaux

Ce sujet est à juste titre très présent dans les médias, car au vu des enquêtes prévues la centralisation dans ce domaine sensible prend de nouvelles dimensions. Se posent surtout les questions de la proportionnalité et de l'anonymisation. Malgré des progrès récemment enregistrés dans ce domaine, un jugement définitif ne peut actuellement pas encore être porté.

Ce n'est que vers la fin de 1996 que l'on s'est rendu vraiment compte, suite à des articles parus dans la presse grand public de l'ampleur de la concentration de données sensibles que représentaient les statistiques médicales prévues par les

hôpitaux. Les indications fournies par la presse sont certainement aussi le fruit de résolutions prises de manière générale par la Fédération des médecins suisses (FMH) concernant les statistiques médicales de la Confédération, et par la Conférence nationale sur la protection des données concernant le traitement de données dans la santé publique. C'est également à la fin de 1996 que le PFPD fut interpellé par les organes cantonaux de protection des données pour donner son avis sur la question des bases légales et de l'anonymisation.
La question de la base légale se pose de manière particulièrement aiguë dans le domaine des statistiques. Car si un traitement est effectué à des fins purement statistiques, les exigences envers les bases légales sont moindres. Ceci peut être justifié par le fait que ces traitements de données sont effectués uniquement à des fins ne se rapportant pas aux personnes concernées. Lors du traitement de données sensibles, il y a lieu cependant de veiller particulièrement au respect du *principe de proportionnalité* lors du traitement de ces données. Ce principe pose certaines exigences envers les rapports entre les actes étatiques et les objectifs poursuivis par ces actes. Avant de pouvoir vérifier si ces exigences sont remplies, il faut d'abord définir de manière aussi claire que possible les objectifs poursuivis par les actes étatiques. Dans ce cadre, il y a également lieu de vérifier si les objectifs visés ne sont pas déjà poursuivis ou ne pourraient pas mieux être poursuivis par d'autres moyens. On s'intéressera ici surtout aux rapports avec les autorisations prévues à l'article 321bis CP pour la recherche dans le domaine de la médecine ou de la santé publique.
Le problème de *l'anonymisation* ne se pose qu'en deuxième lieu. Il devient d'actualité s'il découle des objectifs visés que des critères devant être saisis permettent de conclure à l'identité des personnes concernées. Ensuite, le problème de l'anonymisation doit être vu sous deux aspects. Le premier concerne le «code de liaison» qui devrait permettre de saisir ce que l'on appelle des hospitalisations multiples. Ce code devrait être créé à partir de données d'identification d'un patient, sans pour autant permettre de l'identifier. En ce qui concerne la génération de ce code, des améliorations ont été apportées entre-temps au concept provisoire élaboré en avril 1996. Il n'est pas possible actuellement de porter un jugement sur cette méthode, étant donné que nous ne possédons pas encore assez d'informations concernant certains aspects essentiels de ce système. Nous ne savons entre autres pas encore quels procédés (quelles fonctions hash) et quelles informations seront utilisés pour générer ce code. Le deuxième aspect de l'anonymisation concerne l'ensemble des critères saisis, car il est possible en combinant plusieurs critères (par ex. la date de naissance exacte et le numéro postal d'acheminement du lieu de domicile) d'identifier les personnes concernées, même si chaque critère pris isolément ne permettait pas de le faire. De telles possibilités doivent être évitées à l'aide de ce que l'on appelle des généralisations (par ex. année de naissance à la place de la date de naissance, la région où habite la personne au lieu de la localité) chaque fois que cela est possible sans pour autant trahir les objectifs de la statistique. Cette démarche fait donc également appel au respect du principe de proportionnalité.

6.3 Hospitalisation hors canton - communication de données médicales aux organes cantonaux décidant de la prise en charge des frais

Le PFPD n'est pas compétent pour trancher la question de l'admissibilité de ces communications de données. Étant donné que cette question concerne la Suisse entière,

il a quand même pris position à ce sujet après s'être entretenu avec le groupe de travail des organes cantonaux de protection des données. Même s'il est établi que les organes cantonaux décidant de la prise en charge des frais ont un intérêt à ce qu'on leur communique ces données, les bases légales font défaut.

Le problème soulevé ici se pose suite aux accords qui stipulent qu'un hôpital cantonal peut appliquer un tarif plus élevé pour les patients domiciliés hors du canton que pour les patients habitant le canton. Conformément à l'article 41, 3e alinéa, LAMal, le canton de domicile du patient doit dans ces cas payer la différence entre les coûts facturés et le tarif appliqué par l'hôpital pour les habitants du canton, pour autant que le traitement ait eu lieu dans l'autre canton pour des *raisons médicales.* Ces raisons médicales existent dans les cas d'urgences ainsi que pour les traitements qui ne sont offerts par aucun hôpital de ce canton ni dans aucun autre établissement hospitalier figurant sur la liste des hôpitaux pour ce canton. Pour donner suite aux efforts compréhensibles du canton de domicile de ne pas devoir payer cette différence, il est évident que ce dernier a un intérêt à ce qu'il puisse nier l'existence de raisons médicales. C'est la raison pour laquelle le canton s'efforce de se procurer les informations appropriées.
Étant donné que la communication de ces données se fait d'une institution cantonale (hôpital) à un organe cantonal (responsable de fixer la prise en charge), le PFPD n'a pas la compétence de porter un jugement sur cette question. Cette question concerne pourtant toute la Suisse et le PFPD a été interpellé à ce sujet par la Conférence des directeurs cantonaux des affaires sanitaires ainsi que par divers établissements hospitaliers. Après avoir discuté du problème avec le groupe de travail des autorités cantonales de surveillance de la protection des données, nous avons pris position sur la question de savoir si la LAMal autorise ces communications de données.
La LAMal proprement dite ne mentionne aucune autorisation explicite, pour les cantons, de se procurer de telles informations. Même une obligation des établissements hospitaliers n'est pas contenue dans la LAMal, ni dans l'ordonnance qui s'y rapporte. Se pose donc la question de savoir si un canton est en droit d'édicter lui-même de telles dispositions. Les dispositions de la LAMal visent à inciter les cantons à coordonner la planification et l'utilisation de leurs ressources hospitalières plutôt que de dépenser beaucoup d'énergie pour la démarche complexe de la procédure de prise en charge des frais. Ceci montre clairement que la LAMal ne veut pas fournir de base légale pour la communication de données aux organes cantonaux chargés de la prise en charge des frais. D'un autre côté, il apparaît clairement que des accords valables pour l'ensemble de la Suisse, qui rendraient superflues les procédures de prise en charge, ne peuvent pas être élaborés à court terme. Nous avons donc renoncé à émettre des recommandations directes aux organes concernés. Nous nous sommes restreints à donner des conseils permettant d'améliorer la protection des données lors de la communication de ces dernières. Nous avons en premier lieu insisté sur le fait que des informations médicales ne devraient pas simplement être adressées aux collaborateurs d'une administration, mais que ces données devraient plutôt être réservées aux personnes qui font partie du corps médical ou de son personnel auxiliaire, et qui ont l'habitude de traiter ce genre de données.

6.4. Droit de recevoir des renseignements de l'Office fédéral des assurances sociales vis-à-vis des autorités cantonales (surveillance des caisses)

Certains cantons doutent que l'augmentation des primes des caisses-maladie approuvée par l'Office fédéral des assurances sociales (OFAS) soit justifiée dans leurs régions. Ils désirent donc participer à la procédure d'autorisation de l'OFAS et demandent à cet office de pouvoir consulter les dossiers des caisses-maladie (budgets annuels concernant les régions à l'intérieur des cantons). La transmission de ces données par l'OFAS aux cantons ne repose néanmoins - à notre avis - sur aucune base légale dans la loi sur l'assurance-maladie (LAMal).

L'Office fédéral des assurances sociales a demandé à l'Office fédéral de la justice (OFJ) d'établir si et dans quelles conditions la transmission des dossiers mentionnés par l'OFAS était autorisée du point de vue de la protection des données. L'OFJ a conclu à la nécessité d'une base légale. Il estimait toutefois que l'actuelle loi sur l'assurance-maladie (LAMal) offrait une base suffisante pour que la transmission des données puisse être réglementée, même par voie d'ordonnance. En dernier lieu, l'OFJ nous priait de donner notre avis.
Selon la loi sur la protection des données, la transmission de budgets annuels par l'OFAS aux cantons nécessite une base légale. Contrairement à l'OFJ, nous estimons toutefois que la LAMal ne contient pas de disposition qui autoriserait cette transmission par l'OFAS par voie d'ordonnance. Nous demandons que la LAMal contienne au moins une disposition qui circonscrive le plus clairement possible le but, l'objet ainsi que le volume de la délégation à l'OFAS (norme de délégation). De notre point de vue, une telle disposition ne figure pas dans la LAMal.
On peut même se demander s'il ne faudrait pas réglementer ce point de manière complète et exhaustive dans la LAMal. L'échange d'informations entre l'OFAS et les cantons peut mener à une ingérence grave dans la sphère juridique des caisses-maladie. En effet, les cantons comparent alors les données reçues à leurs propres coûts de santé, puis transmettent leurs observations à l'OFAS, lequel - parfois en s'appuyant sur ces données - autorise ou non les tarifs de primes. Les cantons courent toutefois le risque de ne pas reproduire ou ne de pas pouvoir reproduire correctement le montant des coûts annuels de santé et d'en tirer de fausses conclusions. Les caisses-maladie seraient dans ce cas accusées à tort de subventions non-autorisées. En outre, durant la procédure d'autorisation, les cantons pourraient manquer de l'objectivité et de la neutralité nécessaires. Dans de nombreux cantons, le coût des soins hospitaliers est très élevé et de ce fait, ce sont les cantons qui sont jusqu'à un certain point responsables des très fortes augmentations de primes. Une participation des cantons à la fixation des primes ou leur «cosurveillance» requiert donc au moins une norme de délégation claire dans la LAMal. La surveillance des caisses-maladie - dont fait partie l'approbation des tarifs de primes - revient de toute manière au Conseil fédéral, donc à l'OFAS, et non pas aux cantons.
La question de savoir si et dans quelle mesure la transmission des données d'assurance par l'OFAS aux cantons est autorisée du point de vue de la protection des données doit certes être considérée du point de vue juridique, mais aussi du point de vue politique.
Un «sommet des assurances-maladie» réunissant tous les intéressés s'est tenu à la mi-février 1997. Il a été décidé à cette occasion d'associer les cantons au contrôle des primes. Dans les faits, cette décision se traduira par une modification de l'ordonnance qui sera probablement déjà en vigueur pour la fixation des primes 1998.

6.5. Vente d'un cabinet dentaire (Goodwill)

La personne qui reprend un cabinet dentaire n'est pas autorisée à consulter le dossier médical d'un patient tant que ce dernier n'y donne pas son consentement. Il n'est pas permis non plus à la personne qui remet son cabinet de promettre un tel droit de consultation dans le contrat de vente.

Dans le cadre d'une remise de cabinet, le PFPD a été interpellé pour savoir dans quelle mesure l'acquéreur d'un cabinet dentaire était autorisé à consulter les dossiers existants des patients. En principe, on admet que seul le patient décide de ce qu'il advient des informations qui le concernent. Ceci signifie que c'est lui qui doit prendre cette décision. D'autre part, le nouvel acquéreur doit bien pouvoir consulter le fichier d'adresses s'il veut informer les patients qu'il a repris le cabinet, à moins que l'ancien propriétaire ne l'ait déjà fait. La consultation du fichier d'adresses d'un cabinet dentaire a été jugée admissible du point de vue du secret médical (dans d'autres domaines plus sensibles tels que par ex. en psychiatrie, oncologie ou urologie, ceci serait peut-être jugé différemment). Le vendeur n'est pas en droit de promettre l'accès aux dossiers médicaux dans le contrat de vente, étant donné qu'en sa qualité de *porteur* du secret il est tenu de ne pas divulguer ces informations. Seul le patient en qualité de *maître* du secret peut autoriser la communication à des tiers. Il peut donner ce consentement soit de manière explicite, soit de manière implicite en faisant entendre qu'il aimerait se faire traiter par le dentiste qui reprend le cabinet.

6.6. Questionnaires médicaux et consentement du patient en vue de l'encaissement

Lorsqu'un médecin requiert le consentement de son patient pour communiquer des données le concernant à des fins d'encaissement ou de comptabilité, il doit utiliser pour cela une feuille séparée, à part des questions médicales. La déclaration de consentement à des fins de comptabilité doit permettre de savoir quelles données sont transmises à qui et dans quel but.

Un particulier a été prié, chez son médecin, outre de répondre à des questions d'ordre médical, de signer sur la même feuille une déclaration par laquelle il consentait notamment à la transmission de données le concernant en vue de l'établissement des factures, de l'encaissement et de la comptabilité. Cette personne était gênée par le fait que ce faisant, elle consentait non seulement à la transmission de données comptables générales, mais aussi de données relatives à sa santé.
Il convient en l'espèce d'établir une distinction fondamentale entre les différentes catégories de données personnelles (établissement de la facture et données relatives à la santé). Il ne faut collecter que les données qui sont nécessaires et aptes à atteindre un but déterminé (principe de proportionnalité). Certes les questions d'ordre médical touchent largement la sphère personnelle du patient, mais elles nous semblent aptes à favoriser la qualité du traitement médical. Néanmoins le patient a dans tous les cas le droit de ne pas répondre à certaines questions.
La clause de consentement doit être claire et sans équivoque. La personne qui consent au traitement de ses données ne doit pas seulement y consentir librement, mais aussi en connaissance de toutes les circonstances qui entourent l'ensemble du traitement. Dans le cas présent, le patient devrait pouvoir y trouver le nom des destinataires de ses données (bureau d'encaissement, entreprise de comptabilité,

autres personnes ou institutions mandatées). La mention de ces données ne devrait poser aucune difficulté puisque le médecin connaît le destinataire des données.
Le médecin compléta dans ce sens la déclaration présentée au patient. Du fait de sa formulation standard, donc de son manque de transparence, la déclaration soumise au patient pour signature aurait dû être considérée comme nulle.

7. Crédits

7.1. La gestion de systèmes de contrôle des crédits

Les informations sur la solvabilité ne doivent pas être combinées à un registre par branche permettant de consulter online la liste de toutes les personnes concernées. Du point de vue technique, un système de contrôle des crédits doit être conçu de sorte que la consultation ne soit possible qu'au cas par cas. L'introduction du nom et/ou de l'adresse devrait suffire pour obtenir les renseignements souhaités. Il est également interdit d'envoyer une récapitulation sommaire des mauvais payeurs.

Conformément à la recommandation du PFPD du 24 octobre 1994, on ne peut obtenir des renseignements en matière de crédits que sur demande et de cas en cas. La transmission globale par liste d'informations sur la solvabilité ou les réponses à des questions générales sans motif particulier sont donc exclues (FF 1988 II 468).
A la suite de la recommandation du préposé fédéral à la protection des données, une association a mis en place à l'intention de ses membres un système informatique «Débiteurs», accompagné d'un règlement. Le but était de leur permettre de recueillir au cas par cas des informations sur la solvabilité de leurs clients. Or, du point de vue informatique, les critères de recherche n'étaient pas configurés de manière optimale. Etant donné la lenteur de consultation, les membres de l'association ne pouvaient obtenir aisément les informations souhaitées sur la solvabilité de leurs clients. Pour cette raison, l'association avait l'intention de les informer en leur envoyant une récapitulation sommaire des mauvais payeurs, et en leur donnant ensuite la possibilité de consulter l'index.
Dans la recommandation mentionnée, nous nous sommes déjà prononcés contre l'envoi de listes de mise en garde en matière de crédits. L'envoi à tous les membres d'une association de listes de clients confrontés à des difficultés financières - listes en partie totalement inutilisées - va à l'encontre du principe de proportionnalité. On ne peut faire valoir un motif justificatif qui légitimerait ce traitement. Par conséquent, ce genre de traitement de données personnelles doit être qualifié d'injustifié.
En outre, l'association avait proposé de mettre à la disposition de ses membres un registre par branche sur CD-Rom, rassemblant l'ensemble des clients (environ 2300 personnes) et mentionnant leurs noms et adresses. Ce registre aurait été relié à des données qu'auraient livrées les membres à une centrale (obligation réglementaire des membres). Seuls les membres auraient eu accès au système et moyennant finance, auraient pu ainsi contrôler la solvabilité de leurs clients potentiels. Ces membres se seraient engagés par contrat à ne se renseigner que sur les clients entrant en ligne de compte pour la conclusion éventuelle d'un contrat.
Nous estimons que s'il peut accéder à des informations en matière de crédits, chacun des membres de l'association n'a pas l'intention de conclure un contrat avec toutes les personnes figurant dans le registre et n'a donc pas besoin d'obtenir (surtout online) les informations en matière de crédits concernant tous les clients

potentiels. Le risque que des personnes non autorisées consultent des informations en matière de crédits figurant dans le registre est à notre avis très grand et ne peut être suffisamment réglementé par contrat (problèmes de preuve en cas d'abus). Nous avons donc demandé que la consultation de cas en cas des informations concernant la solvabilité soit réalisée au moyen de mesures techniques appropriées. Chaque membre devrait avoir la possibilité d'obtenir l'information souhaitée en introduisant le nom du client, son adresse ou le numéro TVA (taxe à la valeur ajoutée). Si une entreprise porte différents noms ou possède plusieurs filiales, une seule opération d'interrogation devrait permettre d'obtenir les informations recherchées.
Dans l'état actuel des choses, il a été décidé de ne pas réaliser le nouveau système informatique projeté ni d'envoyer une récapitulation sommaire des mauvais payeurs aux membres de l'association.

7.2. Nouvelles cartes de crédit et signature digitalisée

La digitalisation des signatures a pour but de garantir l'identification des personnes concernées. Elle sert également de protection contre les falsifications. L'entreprise qui désire digitaliser des signatures doit néanmoins en informer auparavant ses clients et recueillir leur consentement. Si cette mesure implique d'autres modifications, comme la conservation des données ou la modification des conditions générales, les clients doivent aussi en être informés au préalable.

Une personne privée désirait savoir si sa banque était habilitée à renouveler sa carte de crédit et à digitaliser sa signature sans l'en informer au préalable ni requérir son consentement.
La signature est une donnée qui se rapporte à une personne déterminée, raison pour laquelle son traitement est soumis à la LPD. 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. La digitalisation de la signature du client constituait en l'occurrence un traitement de données plus large qu'il avait été convenu dans la demande de carte et dans les conditions générales. Les personnes concernées auraient donc dû être informées au préalable de modifications éventuelles afin de donner leur consentement à la digitalisation de la signature. Par conséquent l'attitude de la banque ne répondait pas aux principes généraux de la LPD. En outre, il reste à examiner si ces mesures, du point de vue technique, sont nécessaires et propres à assurer les mesures de sécurité visées.
Indépendamment de la nécessité et de l'opportunité de la mesure visant à garantir l'identification de la signature d'un client, la manière de procéder dans le cas présent n'est pas conforme à la protection des données car elle a eu lieu sans que le client soit informé. Les personnes concernées doivent aussi être informées de la manière dont les données sont conservées.

7.3. La communication à grande échelle de données ZEK à la police des étrangers

Le centre d'informations de crédit (ZEK) a à plusieurs reprises reçu des demandes de renseignement de la part des autorités de police des étrangers. La question s'est donc posée de savoir dans quelles conditions le ZEK était en droit de communiquer des renseignements.

Lors de la réglementation du séjour d'un étranger, les autorités de police des étrangers sont tenues de tenir compte dans une mesure appropriée de la situation financière d'un requérant. Comme nombre d'étrangers s'adressaient au ZEK en utilisant des formulaires pré-imprimés, la question s'est entre autres posée de savoir si une enquête à grande échelle auprès du ZEK, qui est une association privée, était admissible selon la législation en matière d'étrangers et de protection des données. Dans un avis de droit, nous sommes arrivés à la conclusion que des enquêtes à grande échelle avec la participation du ZEK n'étaient pas admissibles. La question de savoir si dans des cas isolés justifiés, le ZEK était en droit de communiquer des renseignements aux autorités, ne nous a pas été posée. Nous sommes cependant d'avis que ceci devrait être possible pour autant que le destinataire ait absolument besoin de ces données pour accomplir sa tâche légale et qu'il puisse rendre vraisemblable que la personne concernée lui refuse les données par abus de droit. Restent réservés les intérêts prépondérants dignes de protection ainsi que les obligations de garder le secret.

8. Marketing direct

8.1. Traitement de données à des fins publicitaires : non-respect du blocage des adresses

Voir rapport de contrôle p. 173

Le PFPD a rédigé une feuille d'information sur le blocage d'adresses utilisées à des fins publicitaires (voir p. 210)

9. Statistique

9.1. La révision de la loi sur le recensement - Recensement 2000

La Commission de gestion du Conseil national (voir notre 3ème rapport d'activités, p. 163), a chargé le Conseil fédéral de rechercher de nouvelles solutions aux méthodes de relevé du recensement. L'Office fédéral de la statistique a élaboré des propositions de réorientation et de simplification du recensement. Dans le cadre de la consultation des offices, nous nous sommes prononcés sur les modifications proposées et avons émis des critiques sur le projet d'utiliser les donnés du recensement pour mettre à jour les registres de l'administration.

La réalisation des prochains recensements sur la base de registres nécessite la création de bases permettant l'harmonisation des registres communaux. Dans cet esprit, l'Office fédéral de la statistique propose d'utiliser les données personnelles relevées à l'occasion du recensement pour la mise à jour et la correction des registres administratifs des cantons et des communes. En d'autres termes, les données personnelles relevées dans le cadre du recensement et qui ne devaient jusqu'ici être utilisées qu'à des fins statistiques, pourront à l'avenir être également utilisées à des fins administratives.

Le projet de révision de la loi fédérale sur le recensement lèverait l'interdiction introduite en 1990 d'utiliser les données du recensement à des fins se rapportant à des personnes. Déjà à la veille du recensement 1990, des résistances étaient apparues lors de l'introduction des dispositions de protection des données. Néanmoins, le Conseil fédéral considérait alors que seule la finalité stricte des données relevées permettait de limiter et de contrôler efficacement l'utilisation des données du recensement. En effet, la séparation stricte entre les fins statistiques et les objectifs administratifs constitue le principe fondamental des relevés statistiques. En d'autres termes, le citoyen n'a à craindre aucune répercussion des indications fournies dans le cadre d'un relevé statistique.
Le projet de révision brisera le principe sur lequel est fondé la statistique (principe de finalité). La séparation fondamentale entre tâches statistiques et objectifs administratifs sera définitivement abandonnée et le précieux secret de la statistique s'en trouvera relativisé.
Si le secret des statistiques est levé et les données du recensement utilisées à des fins administratives, le citoyen risque de se méfier de toute statistique et fournira éventuellement des indications incomplètes ou fausses. D'une part la qualité et la fiabilité des données du recensement en pâtiront et la statistique officielle aura plus de difficultés à obtenir des données personnelles les plus précises possible grâce au recensement de la population. Par ailleurs, en raison de la relativisation de la protection de la personnalité, les données relevées à l'occasion du recensement risquent d'être utilisées au détriment des personnes concernées. La mise à jour des registres communaux pourrait par exemple permettre de punir les manquements à l'obligation d'annoncer son domicile. Il est cependant une menace plus grande, à savoir que les registres des habitants mis à jour sur la base des données du recensement soient utilisés pour de nombreux autres registres administratifs. Les personnes concernées ne sont alors pas en mesure de déterminer quel service a transmis les données, le cas échéant quelle donnée ou quelle source est à l'origine du préjudice qu'elles encourent.
Nous avons salué le relevé à partir de registres, qui permet de réduire les coûts, ainsi que l'harmonisation des registres des communes. Cette harmonisation est la condition de tout recensement à partir de registres. Mais cela ne doit pas se faire au détriment des personnes concernées, et les registres administratifs ne doivent pas être mis à jour à partir de données statistiques.
A long terme, les recensements seront effectués à partir de registres. Et ainsi que l'a souligné la Commission de gestion dans son rapport au Conseil fédéral, il faut soutenir l'établissement et l'harmonisation des registres cantonaux et communaux. Après élaboration des bases légales nécessaires, les cantons pourront procéder à l'harmonisation ou à l'établissement de registres administratifs. Ceux-ci contiendront des éléments également nécessaires à la statistique et seront à l'avenir utilisés pour le relevé indirect des données de recensement sans qu'il y ait un reflux des données statistiques vers les registres administratifs lors du «processus d'ajustement» (interdiction de reflux). En effet, lors du recensement, le risque est moins dans le relevé des données que dans leur mise à jour et leur combinaison.
D'autres pays européens pratiquant le recensement à partir de registres associent des données provenant de différents registres. Mais le reflux des résultats (correction et mise à jour) du recensement n'est pas autorisé. Ainsi, le recensement est effectué sans que le secret de la statistique ou que la protection de la personnalité ne soient heurtés.

VZ-Personencode

Le choix, à l'occasion du projet de révision de la loi sur le recensement, entre la reprise de données du recensement dans les registres des habitants ou la protection effective de l'individu face aux actes administratifs constitue une décision politique qui doit faire l'objet d'une pesée des intérêts en jeu. Elle ne doit toutefois pas reposer uniquement sur des considérations de rationalité ou d'efficacité. La modification du but initial doit donc aussi tenir compte - outre des coûts et de l'efficacité - de la protection de la personnalité.
Nous ne pouvons approuver une révision de la loi sur le recensement qui affaiblirait le secret de la statistique et la protection de la personnalité. Toutefois si une telle modification devait être adoptée, les droits des personnes concernées et les exigences de la protection de la personnalité devraient être garantis.
Les conditions minimales suivantes doivent donc être remplies :

- informer sans équivoque le public que les données relevées seront également utilisées pour la mise à jour des registres administratifs, parallèlement au recensement;
- formuler clairement la modification du but initial d'utilisation dans la loi sur le recensement. Il convient de définir sans ambiguité les données qui seront utilisées pour la mise à jour des registres et dans quels registres elles seront intégrées;
- limiter dans le temps la mise à jour des registres (maximum 6 mois);
- indiquer clairement sur le formulaire de relevé les données personnelles qui seront aussi utilisées à des fins administratives;
- enfin, les données figurant sur les questionnaires ne doivent pas se traduire par un préjudice pour les personnes concernées (établissement d'une interdiction de préjudice).

S'il est obligatoire de répondre au questionnaire sous peine d'une sanction, la personne concernée ne doit pas subir un préjudice uniquement parce qu'elle a rempli correctement le questionnaire.

9.2 Différence entre le traitement de données à des fins statistiques et à des fins administratives

Pour la personne concernée, il y a une différence majeure entre un traitement de données à des fins purement statistiques et la situation où le traitement des données peut engendrer des mesures concrètes dont elle risque de faire l'objet. C'est pourquoi, dans le deuxième cas, les exigences envers l'existence de bases légales sont plus sévères. Il est admissible de traiter des données administratives à des fins statistiques, mais pas inversément.

Les dispositions de l'article 22 LPD concernent tous les traitements de données *à des fins ne se rapportant pas à des personnes*, les exemples cités pouvant être la recherche, la planification et la statistique. Du point de vue de la protection des données, la nature de tels traitements statistiques de données est précisément qu'ils ne se réfèrent plus à des personnes déterminées. De l'autre côté, nous connaissons les traitements à des fins se rapportant à des personnes, c.-à-d. chaque fois que le traitement des données peut engendrer des mesures ou décisions individuelles à l'encontre de la personne concernée. Par contre, les personnes concernées ne doivent pas avoir peur que les traitements à des fins ne se rapportant pas à des personnes engendrent des atteintes à leur vie privée. C'est pourquoi dans le cas du traitement de données sensibles à des fins ne se rapportant pas à des personnes, on a renoncé à définir des bases explicites dans une loi au sens formel. Dans le

même esprit, il est admissible que des données administratives puissent être dépouillées à des fins statistiques, par contre l'utilisation de données saisies à des fins statistiques pour des buts se rapportant à des personnes est formellement interdite.
Il y a lieu par contre dans le cadre de traitements statistiques de données de respecter certaines règles. Premièrement, les traitements ne doivent en aucun cas être effectués à des fins autres que statistiques, et surtout pas à des fins se rapportant à des personnes. Deuxièmement, les données doivent être rendues anonymes chaque fois que le but du traitement le permet, ce qui nécessite d'autre part que le but statistique soit clairement défini. Troisièmement, la publication des résultats doit être faite sous une forme qui ne permet plus d'identifier les personnes concernées.
Comme exemple concret de différents buts de traitement, nous aimerions mentionner la statistique des données administratives de l'assurance-maladie. Dans ce secteur, les dispositions légales existantes ne permettent pratiquement pas de séparer les traitements à des fins statistiques de ceux à des fins se rapportant à des personnes. Même les documentations accompagnant les traitements de données prévus ne donnent pas d'éclaircissements sur cette question. Les articles 21 à 23 de la LAMal sous le titre «Surveillance et statistique» contiennent des dispositions concernant les deux types de traitement. Cette confusion est problématique, vu que la législation sur la protection des données requiert, pour le traitement à des fins administratives, un niveau normatif et un degré de détail supérieurs que pour le traitement à des fins statistiques. Les concrétisations des traitements de données formulés dans les articles 28 à 32 de l'OAMal ne trouvent leur base légale dans la LAMal que dans la mesure où elles se rapportent effectivement à des traitements de données à des fins statistiques (article 23 LAMal). Si leur validité devait s'étendre au-delà, il faudrait - pour satisfaire aux exigences de la protection des données - étendre la norme d'autorisation dans la LAMal. Sous la pression des coûts qui règne dans le secteur de la santé publique et étant donné qu'une révision de loi peut durer très longtemps, on peut pour l'instant se contenter de définir de manière aussi claire que possible les différents buts de traitement. Ceci permet d'obtenir assez de clarté et de transparence pour convaincre les assureurs qu'ils peuvent communiquer certaines données à l'Office fédéral des assurances sociales.

10. Droit de bail

10.1. Formulaire d'inscription pour les locataires

Nous avions transmis en son temps à la Commission fédérale de la protection des donnés notre recommandation sur les possibilités, pour les bailleurs, de collecter des données concernant les locataires potentiels d'un appartement. La Commission nous a communiqué sa décision. Comme nous, elle estime qu'on ne peut collecter sans restriction des informations sur les personnes s'intéressant à un appartement. Pour ce qui est de l'admissibilité de certaines questions en vertu de la protection de données, l'accord ne règne cependant pas sur tous les points.

Voici en résumé quelles ont été les considérations émises par la Commission:
Les questions portant sur le nombre, l'âge et le sexe des enfants sont considérées comme généralement permises, contrairement à ce qui figure dans la recommandation, parce que ces données peuvent faciliter tant la sélection préalable de

l'appartement adéquat pour les personnes qui recherchent un logement, qu'inversément une sélection préalable de personnes intéressées par un appartement précis. Néanmoins, la collecte de données concernant des personnes adultes qui vivent dans le même ménage, mais sans être parties au contrat, n'est possible - comme le précise notre recommandation - qu'en présence de conditions particulières (existence d'un devoir légal, objectif statutaire de la régie immobilière, présence d'autres motifs importants).
Dans sa décision, la Commission a confirmé que la question sur le revenu annuel - admise aux termes de la recommandation - par tranches de 10 000 francs jusqu'à un plafond de 100 000 francs suffit pour estimer la situation financière de locataires potentiels. Cependant, les données ponctuelles sur la situation financière qui ne sont pas aptes à donner une image complète de la situation économique des personnes en question ne doivent pas être demandées (par ex. questions portant sur des contrats de paiement par acomptes et cessions de salaire). En revanche, la Commission considère que du point de vue de la protection de la personnalité, la question du nombre de voitures ne pose aucun problème. En effet, ces renseignements peuvent avoir une importance pour les deux parties au contrat (nombre de places de stationnement disponibles).
La Commission a enfin confirmé que la connaissance de l'état civil n'est nécessaire qu'en présence de conditions particulières.
Par contre, la question de la nationalité (Suisse/étranger) est considérée comme généralement admise car elle peut avoir des répercussions sur la relation avec les autres locataires. Une question plus précise, par exemple sur la catégorie de permis de séjour accordée, n'est pas autorisée dans le cadre d'une sélection préalable.
Notre recommandation selon laquelle le bailleur doit obtenir l'accord du locataire potentiel pour recueillir des références a été estimée adéquate. Néanmoins, le droit à l'information doit se limiter à la confirmation des données figurant sur le formulaire. La Commission recommande donc pour sa part d'adjoindre la mention «facultatif» à cette rubrique. Il en va de même des questions portant sur le lieu de travail, le nom et l'adresse du bailleur actuel. Par contre on ne peut demander l'adresse et le numéro de téléphone de l'employeur qu'en vue de la conclusion du contrat.
Selon la Commission, la collecte des données dans le contexte de listes d'attente qui ne se rapportent pas à un objet particulier doit être possible dans la même mesure que pour les inscriptions à propos d'un appartement déterminé. Une limitation aux nom et adresse ainsi que nous l'avons recommandé dans ce cas ne se justifie pas parce que la tenue de listes d'attente n'a de sens que si elle fournit au bailleur les données nécessaires au choix du locataire à propos d'un logement déterminé. Il convient d'admettre que la présence sur une liste d'attente est en général justifiée par un consentement valable.
Mis à part les diverses questions examinées ci-dessus, la Commission a étudié de plus près et précisé quelques questions fondamentales relevant de la loi sur la protection des données. Elle estime que le PFPD est habilité à émettre des recommandations d'ordre général et abstrait qui vont au-delà du cas concret. Un recours éventuel devant la Commission doit cependant avoir pour objet un destinataire concret.
Le PFPD peut émettre deux sortes de recommandations : celles élaborées dans le cadre de ses fonctions de conseiller (recommandations d'opportunité) et celles qui touchent le domaine du contrôle; ces dernières doivent pouvoir être présentées à la Commission si une violation du droit a été constatée.
La capacité d'émettre des recommandations du PFPD doit être largement interprétée d'après l'art. 29, 1er al., lettre a LPD et ne doit pas se limiter à des er-

reurs de systèmes électroniques d'information. Il convient également de parler d'«erreur de système» au sens de la disposition précitée lorsque le système de traitement est contraire à la loi. C'est le cas lorsque le traitement est apte à porter atteinte à la personnalité d'un grand nombre de personnes.
Enfin, la Commission a précisé les exigences auxquelles doit répondre une déclaration de consentement. La personne donnant son consentement doit pouvoir se décider librement et en toute connaissance des conséquences qui découleront de son consentement. En d'autres termes, il ne faut restreindre ni la liberté contractuelle ni la liberté de décision relative à la communication de données requise dans le cadre de la conclusion d'un contrat. On ne peut donc estimer d'une manière générale que la communication de données a eu lieu sur la base d'une déclaration juridiquement valable.
Néanmoins, c'est sur la base de la situation effective et concrète qu'il convient de décider s'il y a consentement valable. Il est une règle générale : plus les données sont délicates, plus les exigences posées au consentement doivent être élevées.

II. CONTRÔLES DU PFPD

1. Action unique de comparaison de 9000 empreintes digitales entre la Suisse et l'Allemagne à des fins statistiques

Cette comparaison a abouti au résultat que 3,3% des requérants d'asile avaient présenté une demande d'asile aussi bien en Suisse qu'en Allemagne. Un quart des ces requérants «doubles» (c.-à-d. moins de 1% de tous les requérants) sont enregistrés sous un autre nom en Allemagne qu'ils le sont en Suisse. Nous avons participé à une démonstration de la procédure de comparaison et avons été dans les grandes lignes satisfaits de l'organisation et de la sécurité.

Actuellement, en Suisse, on prend et enregistre les empreintes digitales de pratiquement tous les requérants d'asile. Nous avons à plusieurs reprises déclaré que nous considérions cette solution comme disproportionnée et avons demandé d'adopter une démarche plus différenciée, tel que c'est le cas dans d'autres pays d'Europe. Dans ce contexte, nous avons également proposé, de remplacer le terme «doit» de l'article 96 de la loi révisée sur l'asile par le terme «peut». Le résultat de cette comparaison statistique parle en faveur de notre proposition. Il n'est absolument pas vrai que la majorité des requérants d'asile «bombardent» l'Etat de droit en présentant des demandes doubles, comme on veut parfois le faire croire. La vérité est que seule une infime partie des requérants se décide à faire cette démarche. L'analyse statistique ne donne pas de précisions complémentaires concernant les motifs de ces requérants. Si l'on tient compte du fait que seul un quart des 3,3% de requérants «doubles» sont enregistrés sous des noms différents, on peut admettre que les trois quarts restants avaient des motifs honorables. La statistique ne fournit pas non plus d'indication dans quelle mesure les divergences de noms dans les deux pays peuvent être expliquées par les *problèmes bien connus d'orthographe* qui se posent. Cela signifie donc en fin de cause que l'argument souvent avancé de l'abus doit être fortement relativisé. Nous espérons que ceci aura des conséquences sur le travail législatif dans le sens de nos propositions.

Lors de la démonstration de la comparaison à l'Office fédéral des réfugiés nous avons eu dans les grandes lignes une bonne impression de la protection et de la sécurité des données. Nous avons cependant été étonnés qu'on ait voulu nous refuser la commande du système «Impression de la configuration des moyens informatiques utilisés». Le PFPD n'est pas en mesure d'exercer la fonction de contrôle qui lui a été attribuée par la loi s'il n'a pas la possibilité de consulter de manière indépendante les traitements de données et les documentations de traitement devant être contrôlées. Nous avons de même été étonnés de réaliser dans quelle proximité aussi bien organisationnelle que physique les données de police et les données concernant les requérants d'asile étaient traitées. La proposition que nous avons émise sur place à l'adresse des cadres responsables sous forme de recommandation consistant à procéder à une séparation plus nette entre les compétences en matière d'asile et celles de police dans le traitement des données dactyloscopiques a cependant été rejetée.

2. La surveillance des employés au moyen de caméras vidéo

Des systèmes de surveillance à la place de travail (en particulier des caméras vidéo) ne peuvent être utilisées que pour des raisons de sécurité ou pour contrôler le rendement (voir notre 2ème rapport d'activités, p. 138 ss). Dans ce contexte, nous avons examiné un système de surveillance d'une entreprise engagée dans le commerce du papier. Nous n'avons toutefois pas pu constater d'infractions à la loi sur la protection des données.

Suite à l'indication d'un employé, nous avons procédé auprès d'une entreprise bâloise du commerce en gros de papier à un contrôle des caméras vidéo qui y étaient installées. Le système de surveillance se compose de sept caméras vidéo. Celles-ci surveillent les points stratégiques de l'entreprise (point de réception des marchandises, entrée principale et l'accès par ascenseur à l'entrepôt). Les places de travail ne sont pas directement touchées. Les buts poursuivis par la surveillance sont principalement d'éviter les vols, de constater la présence non autorisée de tierces personnes et d'améliorer l'organisation des processus d'exploitation. Une surveillance du comportement des employés ne fait pas partie des objectifs, car la conception simplifiée du système ne se prête pas à ce genre de tâche. Nous avons en outre constaté que le système n'est pas toujours en service. D'autre part, il ne permet pas de mémoriser les images enregistrées pour les traiter ultérieurement. Par ailleurs, on n'utilise pas la possibilité - sans autre existante - de procéder à une écoute des pièces contrôlées. Le personnel a été informé de l'installation des caméras et sur les buts poursuivis et a eu la possibilité de voir lui-même sur les moniteurs quels étaient les champs d'image captés. Nous en avons donc conclus que cette surveillance des locaux du point de vue de la protection des données n'était ni disproportionnée, ni illicite.

3. Traitement de données à des fins publicitaires: non-respect du blocage des adresses

Pour la première fois, une autorité cantonale de protection des données nous a signalé les pratiques publicitaires douteuses d'une maison de vente par correspondance dans le domaine de l'astrologie et de la voyance. Indépendamment de ce fait, nous avons jusqu'ici reçu bien plus de cent lettres émanant de personnes très irritées de toujours recevoir le matériel publicitaire de cette maison malgré des avertissements réitérés. Nous avons donc été amenés d'urgence à examiner la manière dont cette entreprise procédait au traitement des adresses.

Cette entreprise pratique une publicité très intensive pour vendre des produits touchant à la voyance et à l'astrologie. Les adresses proviennent soit d'annonces parues dans la presse, soit sont acquises auprès de diverses maisons de vente par correspondance, surtout de Suisse romande. Comme les mêmes noms figurent souvent dans plusieurs fichiers d'adresses, bon nombre de personnes sont régulièrement importunées par la même publicité. Suite aux prophéties équivoques des divers voyants qui travaillent pour cette entreprise - en réalité il s'agit d'horoscopes standardisés établis par ordinateur - une opposition est apparue en Suisse romande à l'encontre de ces envois publicitaires.
Nous avons visité l'entreprise en question et avons constaté qu'il n'existait qu'un seul fichier clientèle et que les envois refusés ou les blocages d'adresse n'avaient pas été saisis. Nous avons donc sommé l'entreprise de combler cette lacune dans un délai déterminé. Elle nous assura qu'à l'avenir elle confronterait d'abord tout envoi publicitaire à la liste des adresses bloquées. Or nous avons quand même continué à recevoir des réclamations de la part de personnes à qui cette entreprise envoyait encore sa publicité bien qu'elles aient annoncé le blocage de leur adresse. Nous avons donc décidé de procéder à des contrôles supplémentaires et plus précis. Au cas où le système de liste des adresses bloquées ne fonctionnerait pas suffisamment bien, nous avons laisser entrevoir à l'entreprise la possibilité d'une interdiction provisoire de traitement des données jusqu'à élimination du vice.
Lors du second contrôle, nous avons reçu des informations plus précises sur l'organisation et le mode de travail de l'entreprise. Nous avons en particulier contrôlé si le nouveau fichier de blocage des adresses était complet. Nous avons dû constater à notre regret que certaines des adresses qui nous avaient été annoncées comme bloquées ne figuraient pas dans le fichier en question. Le directeur nous expliqua que c'était dû au fait que le traitement des annonces de blocage prenait environ un mois à partir de leur entrée. Il nous assura cependant qu'il veillerait à la mise à jour immédiate du fichier de blocage des adresses. Quant à la suite de la procédure, il fut tenu compte du fait que l'entreprise était régulièrement inscrite dans le registre des fichiers et avait fait preuve d'une volonté de coopération en mettant en place un fichier de blocage des adresses. Nous lui avons donc fixé un dernier délai pour compléter son fichier de blocage des adresses ainsi que pour informer par écrit les personnes concernées. Le directeur nous a entre temps confirmé que suite avait été donnée à notre demande.
Ce cas montre concrètement comment des envois publicitaires indésirables peuvent se transformer en véritable fléau pour les personnes concernées. Notamment les personnes âgées et les personnes crédules se trouvent démunies face aux prophéties malvenues de bonheur ou de malheur et autres rappels opiniâtres. La publicité adressée est un phénomène de notre temps. Elle constitue une forme autorisée d'acquisition de nouveaux clients. Mais lorsque quelqu'un ne souhaite pas

ce genre de publicité, il faut dans l'intérêt de tous les participants trouver les moyens pour que la volonté des clients potentiels soit respectée. A cet endroit, nous aimerions souligner que les possibilités actuelles de blocage des adresses (PTT et liste Robinson) ne suffisent manifestement pas. Il faut donc absolument informer les firmes concernées elles-mêmes de leur obligation de tenir compte des adresses bloquées.

4. Traitement de données concernant des étrangers dans les représentations suisses à l'étranger et aux postes frontières

Les représentations suisses à l'étranger ainsi que les postes frontières traitent également un grand nombre de données personnelles. Lors de deux contrôles effectués à Fribourg-en-Brisgau et dans la région frontalière de Bâle nous avons eu une bonne impression de la protection des données qui y est appliquée.

A l'occasion de deux contrôles effectués en 1996, nous avons eu la possibilité de nous rendre compte comment s'effectuent les traitements de données lors de la délivrance de visas dans une représentation suisse à l'étranger (le consulat de Fribourg-en-Brisgau, fermé entre-temps) et à divers postes frontières dans la région de Bâle. Ces autorités délivrent les visas manuellement. Avant de le faire, ils consultent le Moniteur suisse de police et en cas de doute l'Office fédéral des étrangers à Berne, qui procède aux recherches complémentaires éventuellement nécessaires. Les postes frontières disposent depuis peu de temps d'un accès (restreint) au système de recherches RIPOL, au Registre central des étrangers RCE et désormais également aux données concernant des requérants d'asile disponibles dans AUPER. Les représentations suisses à l'étranger par contre ne disposent pas de tels accès (à l'exception de quelques grandes ambassades qui ont un accès direct au système RIPOL).
Nos contrôles des traitements de données auprès du consulat suisse à Fribourg-en-Brisgau se sont déroulés de manière positive et n'ont donné lieu à aucune critique.
Nos contrôles auprès des postes frontières de la région de Bâle se sont également déroulés de manière positive. Les consultations du RIPOL qui ont été contrôlées étaient en accord avec l'ordonnance RIPOL. Quant aux consultations du RCE contrôlées, nous avons proposé de codifier les motifs de renvoi affichés à l'écran. Lors du contrôle, le système AUPER n'était pas encore opérationnel. Nous avons également suggéré d'une part de procéder aussi vite que possible à l'analyse de sécurité conformément aux directives de sécurité de l'Office fédéral de l'informatique, appréciation qui n'avait pas encore été effectuée au moment du contrôle, et d'autre part de procéder à un cryptage des données sensibles sur les équipements électroniques, pour autant que cela ne soit pas déjà le cas. En ce qui concerne les traitements contrôlés des données de visas et les rapports de contrôle frontière (tous les deux sous forme papier), nous avons trouvé qu'ils étaient conforme aux normes de protection des données.

5. La nouvelle carte d'identité 1995

Depuis le 1er juillet 1994, la nouvelle carte d'identité suisse (CI) est disponible. L'établissement de cette carte ainsi que les conditions régissant le traitement de données personnelles sont stipulés dans l'ordonnance du Conseil fédéral concernant la carte d'identité. Dans la période allant d'octobre 1995 à mars 1996, nous avons vérifié l'application des exigences de protection des données.

Les conditions pour l'établissement de la CI ainsi que le traitement de données personnelles qui en résulte sont régis par l'ordonnance sur la carte d'identité suisse du 18 mai 1994. Entre octobre 1995 et mars 1996, nous avons vérifié l'application des exigences de protection des données. Les aspects essentiels du contrôle portèrent sur le contenu et le caractère isolé de la base de données gérée par l'Office fédéral de la police (OFP), les droits d'accès, la saisie des données, la communication des données au fabricant de la carte et à l'OFP, le traitement des données, en particulier la destruction des données après expiration du délai de conservation, l'utilisation du code lisible par machine ainsi que les informations contenues sur la carte d'identité proprement dite.
De manière générale, nous avons pu constater que les traitements de données effectués par l'OFP ainsi que par le fabricant de la carte satisfont aux exigences de l'ordonnance.
Le Département fédéral de justice et de police n'a cependant pas satisfait à son obligation d'émettre des directives sur les exigences en matière de sécurité des données. D'autre part, nous avons dû constater que le délai de dix jours après lequel le fabricant de la carte est tenu de détruire toutes les données mémorisées n'est pas respecté.
Des mesures ont été prises entre-temps qui assurent que les données auprès du fabricant de carte sont détruites de manière électronique après dix jours. Par contre, l'élaboration de directives relatives aux exigences envers la sécurité des données n'a toujours pas été engagée.
Finalement, nous tenons à relever le fait que ce contrôle a pu se dérouler dans un excellent climat de coopération.

III. AUTRES THEMES

1. Publication de données personnelles

1.1. Publication de données concernant des hooligans dans le journal «Sport»

Le journal «Sport» a publié le nom, l'adresse et la date de naissance de personnes qui étaient frappées d'une interdiction de stade prononcée par la Commission de discipline et de sécurité de la Ligue nationale de l'Association suisse de football.

Le journal «Sport» a publié le nom, l'adresse et la date de naissance de personnes qui étaient frappées d'une interdiction de stade prononcée par la Commission de discipline et de sécurité de la Ligue nationale de l'Association suisse de football. Le nom, l'adresse et la date de naissance sont des données personnelles au sens de la LPD. La condamnation par un tribunal public constitue une donnée personnelle

sensible au sens de la LPD. Nous avons défendu le point de vue qu'une interdiction de stade prononcée par la Commission de discipline et de sécurité de la Ligue nationale de l'Association suisse de football exerçait un effet similaire sur la considération sociale de la personne concernée qu'une condamnation par un tribunal public. C'est la raison pour laquelle une interdiction de stade doit être considérée comme donnée sensible et doit donc bénéficier d'un haut degré de protection.
La publication du nom, de l'adresse et de la date de naissance de personnes étant frappées d'interdictions de stade ne peut avoir lieu que si elle est justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public ou par une loi. Une publication, donc une communication des ces données personnelles aux lecteurs du journal «Sport» et ainsi au public n'est justifiée par aucune loi et ne peut également pas être justifiée par un intérêt privé ou public. Par contre, la communication des données personnelles aux organes chargés de la sécurité et de l'ordre dans les stades et dans leur entourage serait justifiée. Afin de respecter le principe de proportionnalité, il n'est cependant pas opportun de distribuer des listes complètes de toutes les personnes frappées d'interdictions de stade aux organes de sécurité de tous les stades. Il y a lieu plutôt de communiquer ces données personnelles uniquement aux organes chargés de la sécurité dans les stades pour lesquels l'interdiction de stade a été prononcée.

1.2. Publication d'un rapport sur les avoirs des victimes du nazisme

L'information du public et l'intérêt historique ne justifient pas que l'on publie un rapport sur les avoirs des victimes du nazisme et les accords avec les pays de l'est en maintenant les noms de l'ensemble des personnes concernées. La protection de la personnalité et des droits fondamentaux nécessite que le rapport soit anonymisé dans une large mesure avant d'être publié. Seuls les noms des personnes physiques et morales ayant un rôle public déterminant peuvent être publiés.

L'avis du PFPD a été requis au sujet de la publication du rapport de deux historiens mandatés par le DFAE pour faire la lumière sur les avoirs des victimes du nazisme et les accords de dédommagement avec les pays de l'est. Le rapport a notamment pour but de faire la lumière sur le comportement des autorités politiques et administratives suisses dans l'affaire des avoirs déposés en Suisse par les victimes des nazis et des indemnisations de biens nationalisés grâce à des accords entre la Suisse et des pays de l'est européen. Le rapport contenait le nom de nombreuses personnes décédées ou encore en vie (conseillers fédéraux, ministres, ambassadeurs, directeurs, fonctionnaires, banquiers, personnes concernées par les fonds en déshérence, avocats, etc.) et des informations relatives à ces personnes, notamment des déclarations ou prises de position. Dans la mesure où ces informations se rapportent à des personnes encore en vie, il s'agit de données personnelles soumises à la loi fédérale sur la protection des données. Quant aux personnes décédées, la protection de leur personnalité s'arrête en principe au moment de leur mort. Demeure cependant réservée la protection de la personnalité dont jouissent les proches.
Il s'agit en grande partie d'une recherche qui ne se réfère pas à des personnes concernées et dont les résultats devraient être publiés sous une forme ne permettant pas d'identifier les personnes concernées. Une partie de la recherche se réfère cependant à ces dernières puisqu'elle a pour but d'examiner le comportement de certaines personnalités publiques ayant assumé des responsabilités dans ce dossier

durant la période incriminée. La publication des données relatives à ces personnes relève dès lors de l'article 19 LPD. Au terme de cette disposition, la publication n'est possible que si:

- elle repose sur une base juridique,
- le destinataire a, en l'espèce, absolument besoin de ces données pour accomplir sa tâche légale,
- la personne concernée y a en l'espèce consenti ou les circonstances permettent de présumer un tel consentement, ou
- la personne concernée a rendu ses données accessibles à tout un chacun.

On peut admettre qu'il y a une base juridique, pour le moins implicite, répondant à un intérêt public prépondérant. A l'avenir la question ne se posera plus car depuis le 14 décembre 1996, l'arrêté fédéral concernant les recherches historiques et juridiques sur le sort des avoirs ayant abouti en Suisse à la suite de l'avènement du régime national-socialiste crée une base légale claire pour la publication des résultats des recherches qui seront effectuées par la commission Bergier.

La communication, respectivement la publication sont également soumises au respect des principes généraux du traitement et notamment au principe de proportionnalité. Celle-ci doit ainsi intervenir de manière à porter le moins possible atteinte aux droits fondamentaux et à la personnalité des personnes concernées. En particulier, il faudra tenir compte du fait qu'un tel rapport, de par son importance politique et médiatique, est voué à une large diffusion et qu'il sera selon toute vraisemblance, rapidement disponible sur un site internet en Suisse ou à l'étranger. De ce fait, une grande prudence est de mise avant la publication des noms des personnes concernées. A moins que l'intérêt public soit tel qu'il l'emporte sur l'intérêt à préserver l'anonymat (ce qui en l'espèce n'était pas démontré), il faudrait en particulier éviter la publication du nom de personnes en relation avec des appréciations subjectives, pas absolument fondées, voire contestées. Ainsi, seuls les noms des personnes dont la connaissance est indispensable à la compréhension de faits survenus peuvent être publiés. Il s'agit en particulier des noms de personnes physiques ou morales connues du public (notamment personnalités de la vie publique) et qui ont assumé des responsabilités politiques, économiques, morales et décisionnelles.

Ainsi, le PFPD est parvenu à la conclusion que la plupart des personnes mentionnées dans le rapport pouvaient être rendues anonymes. Il n'était dès lors pas nécessaire en particulier de mentionner au côté des services de l'administration impliqués, les noms des fonctionnaires en charge du dossier, si ceux-ci n'occupaient pas une fonction dirigeante et à ce titre n'étaient pas connus du public. Il en allait de même du nom des personnes victimes des nazis, ainsi que les noms des membres de leur famille ayant entrepris des démarches en vue de retrouver leurs avoirs. Ces personnes dans la mesure où elles vivent encore, n'ont pas nécessairement l'intérêt et le désir de voir leur nom publié et largement diffusé. Enfin, il faudrait renoncer à publier le nom des avocats mandatés par des victimes et leur famille. Par contre, rien ne s'oppose, a priori, à publier les noms des banques impliquées, des conseillers fédéraux, ministres des gouvernements étrangers et directeurs d'office directement impliqués. Il en allait de même des ambassadeurs et hauts fonctionnaires ayant pris part aux négociations, dans la mesure où ces noms étaient absolument nécessaires à la compréhension des faits.

1.3. Publication sur Internet d'arrêts du Tribunal fédéral non anonymisés

Le Tribunal fédéral met à disposition du public un nombre d'arrêts du TF sous forme non anonyme par le biais du réseau Internet. La loi fédérale sur la protection des données stipule qu'une telle communication de données nécessite une base légale.

Nous avons rendu attentif le Tribunal fédéral que nous saluions également un accès plus simple aux arrêts du TF, mais qu'il y avait néanmoins lieu de respecter les conditions-cadre de la loi pour la mise à disposition d'informations.
La loi sur la protection des données (LPD) stipule à l'article 17, 2e alinéa que des données sensibles telles que poursuites ou sanctions pénales (article 3 lit. c LPD) ne peuvent être traitées que si ceci est explicitement prévu par une loi au sens formel. En outre, l'article 19, 3e alinéa, LPD mentionne que des organes fédéraux sont en droit de rendre des données personnelles accessibles par procédure d'appel (par ex. en ligne sur Internet) que si cela est prévu expressément. Les données sensibles ou les profils de la personnalité ne peuvent être rendus accessibles au moyen d'une procédure d'appel que si une loi au sens formel le prévoit expressément. Le but poursuivi par la mise à disposition sur Internet serait également atteint si les données étaient proposées sous forme anonyme. Une telle démarche rendrait également caduque l'exigence d'une base légale du point de vue de la protection des données.

2. Service civil

2.1. Le système de traitement de données du service civil ZIVI

La mise en exploitation du système ZIVI permet de simplifier et de rendre plus efficace l'exécution du service civil. Nous avons donné notre accord à l'ordonnance concernant le système d'information du service civil sous réserve que celle-ci soit révisée d'ici la fin 1998.

Le système d'information ZIVI traite un grand nombre de données sensibles. Celles-ci incluent des données telles que religion, idéologie, appartenance à des groupements ou sectes, chômage, enquêtes disciplinaires, mesures d'aide sociale et santé des personnes astreintes au service civil. Plusieurs organes (organes d'exécution centralisés et décentralisés de l'Office fédéral de l'industrie, des arts et métiers et du travail ainsi que l'Assurance militaire) participent à ZIVI. Des tiers, chargés d'exécuter des tâches en rapport avec le service civil, sont également reliés au système. Parmi ces organes, certains sont directement reliés au système en mode online. La loi sur la protection des données prévoit que de tels systèmes doivent reposer sur une base légale au sens formel. Une telle base légale a été créée avec la loi fédérale sur le service civil. Celle-ci ne prévoit pourtant pas le traitement de données sensibles. La base légale au sens formel du système ZIVI doit donc être adaptée aux exigences de la protection des données lors de la prochaine révision de la loi. Nous avons en outre demandé que l'ordonnance sur le système d'information ZIVI règle explicitement les détails du traitement de données sensibles. En particulier, l'ordonnance devra standardiser les droits d'accès, les organes et tiers impliqués, le but poursuivi par l'accès et son ampleur ainsi que les données concernées. A la date de mise en vigueur de la loi sur le service civil (1er octobre 1996) cette ordonnance ne satisfaisait pas encore aux exigences de la

protection des données. Nous étions cependant conscients du fait que le système devait être mis en service sans tarder, raison pour laquelle nous avons donné notre accord à cette ordonnance à condition que celle-ci soit révisée d'ici la fin 1998.

3. Archives

3.1. Délai de protection pour les données sensibles et les profils de la personnalité dans la nouvelle loi sur les archives

Dans la nouvelle loi sur les archives, le Conseil fédéral a fixé le délai de protection pour les données sensibles et les profils de la personnalité à 50 ans.

Après avoir consulté les offices et engagé une procédure de corapport, le Conseil fédéral a approuvé le message et le projet relatifs à la nouvelle loi sur les archives (voir aussi notre premier rapport d'activités, p. 130 ss) et a fixé le délai de protection pour les données sensibles et les profils de la personnalité à 50 ans à compter de la date du document le plus récent.
A l'origine, nous avions demandé que le délai de protection pour les données sensibles et les profils de la personnalité dure au moins jusqu'au décès de la personne concernée. Cette exigence était basée sur la connaissance que dans d'autres pays, comme l'Allemagne, le délai de protection pour toutes les données personnelles, donc non seulement pour les données sensibles et les profils de la personnalité, dure jusqu'à 10 ans après le décès et qu'en Suisse également le canton de Zurich prévoit un délai de protection pour les données sensibles s'étendant jusqu'au décès de la personne concernée. Nous avions accepté la demande consistant à réduire le délai et nous étions mis d'accord avec les Archives fédérales sur un délai de protection de 70 ans. C'est pourquoi grand fut notre étonnement d'apprendre par la voie des médias que la vaste procédure de corapport avait été close sans que nous ayons été consultés, et que d'autre part le délai de protection avait été réduit de 70 ans à 50 ans.

4. Communication de données personnelles

4.1. La mise à disposition par l'administration fédérale de données relatives à ses employés par procédure d'appel

Il s'agissait à l'origine de constituer un annuaire, accessible par procédure d'appel, à partir du contenu de l'annuaire fédéral et de la liste des téléphones de l'administration générale de la Confédération. La proposition d'ordonnance adoptée par le groupe de travail réglementera l'introduction de recueils d'adresses dans l'administration fédérale.

Ainsi que le précédent rapport d'activités en fait état (p. 135), l'Office fédéral de l'informatique a mis sur pied un groupe de travail réunissant des représentants de la Chancellerie fédérale et de nos services afin d'élaborer une base juridique suffisante pour la mise à disposition de données sur les collaborateurs sous forme d'annuaires (par ex. l'annuaire X.500). Le groupe de travail a été dissout au terme de la mise au

point d'un projet d'ordonnance destiné à la Chancellerie fédérale. En effet, la version définitive de l'ordonnance sera établie dans le cadre de la consultation des offices.
Ce projet contient des dispositions relatives à des recueils d'adresses dans l'administration fédérale. Il règle le but, le contenu, l'accès aux informations, les droits des personnes concernées, le devoir d'information sur les risques et les responsabilités. De même, il a été établi que l'accès au moyen d'une procédure d'appel au niveau "administratif externe" est limité aux interlocuteurs vis-à-vis de tiers (collaborateurs de l'administration fédérale qui servent d'interlocuteurs vis-à-vis du public).

4.2. Communication de données en provenance du fichier des déchets spéciaux de l'OFEFP

Si une autorisation légale suffisante manque, les données d'entreprises traitant des déchets spéciaux ne peuvent être communiquées qu'avec l'assentiment de la société concernée. Si le fichier est transféré chez un tiers, celui-ci doit remplir les mêmes exigences que l'Office fédéral de l'environnement, des forêts et du paysage (OFEFP).

L'OFEFP nous a posé la question si et dans quelles conditions il pouvait transmettre son fichier des déchets spéciaux sur support électronique à une entreprise privée, et si ces données pouvaient être communiquées à d'autres destinataires en Suisse et à l'étranger. Dans notre réponse, nous avons communiqué à l'OFEFP que le fichier en question ne pouvait être transmis à des entreprises en Suisse ou à l'étranger que sur la base d'une autorisation légale explicite ou avec l'accord des entreprises concernées. D'autre part, les destinataires devaient offrir des garanties suffisantes en ce qui concerne un traitement des données sûr et conforme au but fixé. Étant donné que dans ce cas il n'y avait ni autorisation légale ni assentiment des personnes concernées, nous avons considéré ces traitements comme inadmissibles et avons répondu à la question de manière négative.

4.3. Transmission de rapports médicaux détaillés directement aux autorités de police des étrangers

Nous avons été rendus attentifs de la part du corps médical au fait que des médecins ont été à plusieurs reprises incités à mettre à disposition directe des autorités de police des étrangers des rapports concernant des patients étrangers y compris le diagnostic et l'anamnèse. L'instance du médecin de confiance manquait.

Conformément à la législation sur les étrangers, un ressortissant étranger peut séjourner en Suisse pour se soumettre à un traitement médical. Dans la mesure où ce séjour nécessite une autorisation, il est tenu de fournir les renseignements nécessaires à l'autorité compétente en matière d'autorisation. Lorsqu'il s'agit de renseignements détaillés sur la santé de la personne, nous sommes d'avis que ces indications ne doivent être fournies qu'à des personnes qui sont soumises au secret médical (membres du corps médical). C'est à ces derniers de transmettre sous forme succincte le résultat influençant la décision à l'autorité compétente. Ceci garantit que les données se rapportant à la santé de la personne en question soient par principe traitées uniquement par des médecins. Ceci n'empêche pas pour autant d'appliquer la législation sur les étrangers.

Nous continuons à être en rapport avec les autorités compétentes afin d'oeuvrer vers une pratique conforme à la protection des données.

4.4. Communication d'un rapport d'enquête administrative aux commissions de gestion

Conformément à la loi fédérale sur les rapports entre les conseils (LREC), les commissions de gestion des Chambres fédérales peuvent demander la transmission d'un rapport d'enquête. Dans la mesure où ce rapport contient des données personnelles, sa communication est en principe soumise aux dispositions de la loi fédérale sur la protection des données et notamment au respect du principe de proportionnalité. Ainsi, seules devraient être communiquées les données nécessaires à l'accomplissement des tâches légales de surveillance des commissions de gestion. S'il appert notamment que seules les conclusions et les recommandations contenues dans le rapport sont suffisantes ou s'il est possible de transmettre un rapport ne mentionnant pas les noms des personnes concernées, on limitera la communication ou on procédera à une anonymisation - partielle ou totale - du rapport avant sa transmission.

Le DFEP a requis l'avis du PFPD au sujet de la communication d'un rapport d'enquête administrative aux commissions de gestion des Chambres fédérales. Ce rapport parvient à la conclusion qu'un certain nombre d'erreurs et de négligences ont été commises par des fonctionnaires et que certains agissements revêtent un caractère illicite pouvant déboucher sur des poursuites pénales. Le rapport énumère les noms des personnes qui ont été impliquées dans l'affaire en question. Il relate en particulier des faits et des déclarations des personnes concernées. Ces informations, dans la mesure où elles sont reliées avec une personne identifiée ou identifiable, sont des données personnelles. Certaines de ces informations sont de nature sensible puisqu'elles concluent à des agissements illicites justifiant une poursuite pénale ou disciplinaire. Le traitement de ces données personnelles et en particulier leur communication sont soumis à la LPD. Dans le cas d'espèce, la communication n'est possible que si une disposition légale le prévoit ou si le destinataire a absolument besoin des informations pour accomplir ses tâches légales.
Les dispositions de la LREC constituent des dispositions légales suffisantes pour légitimer la communication du rapport d'enquête aux commissions de gestion. Il sera ainsi en principe donné suite à la demande, à moins que la sauvegarde d'un secret de fonction, la sauvegarde d'intérêts personnels dignes d'être protégés ou une procédure en cours non encore close justifient la présentation d'un rapport spécial limitant notamment la communication aux conclusions et recommandations du rapport d'enquête. Lors de la communication éventuelle du rapport d'enquête, il convient également de respecter les dispositions de la LPD et notamment les principes généraux du traitement. En particulier, la communication devra être limitée aux seules informations nécessaires aux tâches de surveillance des commissions de gestion et dans la mesure du possible, les données personnelles seront anonymisées. En outre, sous l'angle de la bonne foi et pour autant que le rapport ne puisse être rendu anonyme, les personnes concernées devraient être informées de la communication. Cette dernière exigence n'a pas pu être remplie pour des raisons de praticabilité.

5. Protection des données et conditions légales cadres

5.1. Traitement de données prescrit par la loi et information des personnes concernées

Informer la personne concernée d'un traitement de données peut faciliter le contact avec le public. Il convient toutefois de veiller à ce que l'on utilise uniquement des données qui sont correctes et à jour. Les données erronées doivent être corrigées.

La révision de la loi sur le droit d'auteur (LDAu, RS 231.1) a permis de déléguer à une personne privée (société de gestion) la compétence de réclamer le paiement de dommages-intérêts pour reprographie. Pour que cette tâche fédérale puisse être remplie, il a fallu que les données nécessaires soient recueillies, traitées et facturées à la personne concernée. Nous avons attiré l'attention de la société de gestion sur le fait que les personnes concernées devaient être informées du traitement de leurs données personnelles (accomplissement d'une tâche de la Confédération par une personne privée, bases légales, état des frais et autres). Néanmoins, les personnes concernées n'ont pas été informées, notamment pas de la possibilité du droit d'accès et de rectification en vertu de la LPD.
Ayant reçu des factures contenant des indications en partie erronées, diverses personnes désiraient savoir qui avait collecté des données erronées sur leur compte. Bien que la provenance des données ne soit pas expressément mentionnée dans la loi, cela ne signfie pas que les tiers mandatés pour recueillir des données ne doivent pas être mentionnés sur demande aux personnes concernées. Le droit d'être informé de la provenance des données découle également de la fonction du droit d'accès, qui est de protéger la personnalité et de garantir les principes démocratiques et constitutionnels. Il ne peut y avoir protection de la source vis-à-vis de la personne concernée qu'en présence d' intérêts prépondérants à conserver le secret conformément à l'article 9 LPD. La restriction du droit d'accès doit être motivée en conséquence.
En droit de la protection des données, une personne privée à qui des tâches publiques de la Confédération sont confiées est considérée comme organe fédéral. Elle doit communiquer à la personne qui le demande toutes ses données personnelles figurant dans le fichier. Si cette personne demande aussi la provenance des données, donc l'adresse des mandataires, il faut si possible les indiquer. La personne concernée a en effet un intérêt légitime à rectifier des données erronées également auprès de tiers. Pour ces raisons, nous avons recommandé au maître du fichier de communiquer l'adresse de l'entreprise (éventuellement après en avoir informé celle-ci) aux personnes à propos desquelles des données erronées avaient été traitées et qui en demandaient la provenance, pour que la rectification nécessaire puisse être requise auprès des services concernés. Si la provenance des données ne peut être communiquée (par ex. source inconnue), la personne privée garantira elle-même à la personne concernée qu'elle veillera à la rectification des données erronées.
Ces deux exemples de rectification de données erronées (par la personne concernée elle-même ou par le maître d'un fichier) montrent comment éliminer le doute suscité par le manque d'information à propos de la provenance et de l'exactitude des données.

5.2. Le droit d'accès et le registre des fichiers

Quiconque veut obtenir des renseignements sur un traitement de données personnelles doit le demander au maître du fichier. Par contre, le PFPD établit et gère un registre public des fichiers traités par des organes fédéraux ou par des personnes privées. Néanmoins, on y trouve non pas des données personnelles, mais uniquement des catégories de données personnelles.

Le préposé fédéral à la protection des données reçoit régulièrement des demandes émanant de personnes privées qui désirent obtenir des renseignements sur des données les concernant. Nous ne pouvons traiter ces demandes car le PFPD tient seulement un registre des fichiers, exempt de données personnelles, et de ce fait ne peut donner aucun renseignement sur le contenu de ces fichiers.
Les quatre premiers volumes du registre du PFPD ont été publiés en 1996 et contiennent les fichiers :
- du Département fédéral de l'Intérieur (A1);
- du Département fédéral des Finances et de la Banque nationale suisse (A2);
- des assurances sociales (A3);
- ainsi que de personnes privées (B1).

Deux autres publications sont prévues pour 1997 (voir p. 197).
Il est conseillé aux personnes qui nous consultent de s'adresser directement au maître du fichier en question. S'il s'agit d'un organe fédéral ou d'une personne privée, on peut faire valoir le droit d'accès conformément à l'article 8 LPD. La personne concernée remet une demande à cet effet et doit prouver son identité (par ex. copie de la carte d'identité ou du passeport). Le maître du fichier lui communique ensuite toutes ses données personnelles, le cas échéant les catégories de données personnelles traitées, de participants au fichier et de destinataires des données. La communication des renseignements ou la décision motivée de limitation du droit d'accès doit avoir lieu dans les trente jours, en règle générale gratuitement. Si ce délai ne peut être tenu, le maître du fichier doit en informer la personne qui a fait la demande et lui communiquer le délai dans lequel les renseignements demandés seront fournis. Cette communication a lieu en général sous forme d'imprimé ou de photocopie des documents en question.
Le registre sert aussi d'instrument de contrôle et peut être consulté par tout un chacun dans le but de vérifier les renseignements livrés par les maîtres de fichiers.
La personne qui désire faire valoir son droit d'accès auprès d'une autorité cantonale doit s'adresser directement au service cantonal compétent.

5.3. Personnes morales et LPD

Les personnes privées qui traitent des données personnelles sont soumises à la LPD. On entend par personnes privées à la fois les personnes physiques et les personnes morales. Les personnes morales sont par exemple les sociétés anonymes, les sociétés à responsabilité limitée, les coopératives, les fondations, les institutions ainsi que les collectivités.

Une personne privée avait remis à une fondation une demande d'accès conformément à l'article 8 LPD. Elle n'obtint pas les renseignements demandés avec pour motif que la fondation n'était pas soumise à la LPD.
Les personnes privées qui traitent des données personnelles sont soumises à la LPD. Néanmoins, il n'est pas toujours facile de déterminer si la personne procédant

au traitement des données doit être qualifiée de personne privée ou d'organe fédéral. Le législateur a utilisé comme critère déterminant la nature juridique de l'activité qui est à la base du traitement des données. Il convient de déterminer de cas en cas si une activité repose sur le droit privé ou public. Une fondation qui réalise des affaires courantes et conclut à cet effet des contrats de location, de travail et de vente est à notre avis une fondation de droit privé au sens du code civil et de ce fait une personne morale soumise à la LPD. Elle est donc tenue de remplir son devoir d'information.
Si les renseignements sont refusés, une action en exécution du droit d'accès peut être ouverte à l'encontre de la personne morale (article 15 LPD).

5.4. Transposition des exigences de la LPD dans la législation

Selon la LPD, des bases légales au sens formel doivent être créées ou adaptées d'ici le 1er juillet 1998 pour les fichiers existants qui contiennent des données sensibles ou des profils de la personnalité. Dans une circulaire adressée aux départements et aux offices fédéraux, nous avons rappelé à la mémoire de ces derniers que cette question était toujours en suspens.

Dans cette circulaire, nous avons également rendu attentif à notre avis de droit publié dans la JAAC 60.77 (voir aussi notre 3ème rapport d'activités 1995/96 p. 171 ss) et avons joint la check-list contenue dans ce rapport (en annexe p. 103).

5.5. L'outsourcing comme exemple de conflit entre le droit de la protection des données et les dispositions contractuelles

Nous avons constaté que les entreprises dans le secteur de l'informatique n'incluent souvent pas les dispositions obligatoires de protection des données dans leurs contrats ou même les excluent explicitement.

Conformément à la loi sur la protection des données (LPD), les entreprises privées doivent également appliquer les mesures de sécurité des données qui sont nécessaires. Dans les contrats d'outsourcing par exemple, il y a lieu non seulement de stipuler que l'entreprise externe n'est pas en droit d'accéder aux données des collaborateurs transférés. Il est également obligatoire de prendre les mesures techniques nécessaires pour par ex. rendre un tel accès impossible. Au cas où un accès aux données devait devenir nécessaire pour l'exécution des tâches déléguées, il incombe de s'assurer que les collaborateurs de l'entreprise externe ne puissent pas interpréter ces données. La reproductibilité du traitement de données par l'entreprise externe mandatée devrait présenter un intérêt pour le mandant. C'est lui qui, en vertu des dispositions de la loi sur la protection des données, est responsable du traitement des données. L'article 14 LPD prévoit que le traitement de données personnelles peut être confié à un tiers pour autant que le mandant veille à ce que ne soient pas effectués de traitements autres que ceux qu'il est lui-même en droit d'effectuer et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdise.

Logarithmus

S'il est possible pour un produit de rendre impossible par des mesures techniques l'accès aux données concernant les clients ou l'interprétation de ces données (pour des personnes non autorisées), ceci augmente considérablement la valeur du produit. Ainsi, on satisfait aux exigences de la protection des données tout en offrant aux clients un produit meilleur et plus utile.

6. Protection et sécurité des données

6.1. La sécurité des données dans l'Administration fédérale

Nous allons décrire ci-dessous comment les mesures de sécurité des données, qui découlent de la protection des données, sont appliquées au sein de l'Administration fédérale et dans quels secteurs il existe encore des différences.

Dans l'Administration fédérale on distingue trois niveaux de protection pour la sécurité des données. Pour le niveau de protection 1, les mesures de sécurité des données sont minimales, pour le niveau de protection 3 elles sont maximales. Du point de vue de la protection des données, les niveaux de protection ont été définis comme suit:
niveau 1: les données à caractère personnel dont l'abus ne semble pas provoquer une atteinte particulière ainsi que les données personnelles librement accessibles au public, telles que les données concernant l'adresse (nom, prénom, adresse, date de naissance), pour autant qu'elles soient neutres et hors d'un contexte sensible;
niveau 2: les données à caractère personnel dont l'abus peut affecter la personne concernée dans sa position au sein de la société ou dans sa situation économique, telles que les données relatives à sa situation de locataire ou celles concernant ses relations professionnelles;
niveau 3: les données à caractère personnel dont l'abus peut gravement affecter la personne concernée dans sa position au sein de la société ou dans sa situation économique; les données qui sont sujettes à un secret de fonction particulier, telles que les fichiers de patients, les données relatives au personnel ainsi que les données sensibles ou les profils de la personnalité; les données à caractère personnel dont l'abus peut signifier un danger pour la vie de la personne concernée, telles que les adresses de témoins dans certaines poursuites pénales.
Du point de vue de la protection des données, le niveau 1 est satisfait en grande partie par les mesures de sécurité de base. Il incombe à l'unité administrative en question d'appliquer elle-même lesdites mesures. Pour les niveaux de protection 2 et 3, les objets de sécurité doivent être annoncés au service de sécurité informatique de l'Office fédéral de l'informatique par le responsable pour la sécurité des départements ou des offices en vue d'obtenir une assistance lors de l'appréciation des risques. Le manuel n° 1 accompagnant la directive S02 relative à la sécurité informatique contient un catalogue complet de mesures, catalogue qui permet selon le niveau de protection de déterminer et d'appliquer les mesures nécessaires. En outre, les propositions de projets informatiques qui seront réalisés au sein de l'Administration fédérale sont remises au Préposé fédéral à la protection des données. Selon la sensibilité de ces projets, ils seront accompagnés par des collaborateurs du Préposé fédéral à la protection des données de manière plus ou moins soutenue pendant les phases de planification, de développement et d'exploitation ou analysés sous l'angle de la protection des données. Les aspects

mentionnés ci-dessus nous ont déjà permis de faire un certain chemin en ce qui concerne la protection et la sécurité des données. Par contre, nous devons souvent constater qu'il est difficilement possible au sein de l'Administration fédérale de s'engager pour une application adéquate des mesures de sécurité des données si l'on ne dispose pas des moyens nécessaires et/ou de bases légales suffisantes pour faire appliquer la sécurité des données et ainsi une partie de la protection des données.
Nous continuons à constater dans les phases de planification des projets que les déroulements (existants/souhaités) ne sont pas ou insuffisamment documentés. L'ordonnance relative à la loi fédérale sur la protection des données (OLPD) stipule à l'article 21 que l'organisation interne des organes fédéraux respectifs doit être documentée. Le guide relatif aux mesures techniques et organisationnelles de la protection des données concrétise en plus que plus le système en question est sensible du point de vue de la protection des données, plus la documentation de l'organisation interne (organisation structurelle et fonctionnelle) doit être détaillée. Nous avions déjà relevé ceci dans notre premier rapport d'activités 1993/94 (p. 146/147). En présence d'une documentation insuffisante sur le système, on ne peut pas parler d'un système transparent. En fait, un tel système n'est ni conforme aux exigences de la protection des données, ni compréhensible et très vraisemblablement compréhensible uniquement pour des collaborateurs de longue date.
Sur la base des réflexions faites ci-dessus et sous l'angle de la protection des données, il est nécessaire d'exiger la transparence adéquate.

6.2. Dépôt de clés

De plus en plus souvent, des données sont cryptées pour éviter qu'elles puissent être interprétées par des tiers. L'interdiction de cryptage demandée par certains organes de contrôle ou le dépôt de clés ne permettent pas de résoudre de manière définitive les problèmes qui se posent pour les autorités judiciaires.

Les personnes privées, les entreprises et l'administration publique aimeraient que leurs données soient traitées de manière confidentielle, intègre et valable. C'est pourquoi on utilise de plus en plus de bons procédés de cryptage lors des traitements automatisés de données. Un désavantage que le cryptage présente aujourd'hui encore est le fait qu'il n'y a pas de système commun de clés applicable à toutes les plates-formes informatiques et que le cryptage nécessite des ressources supplémentaires (coûts, puissance de l'ordinateur). Si l'on tient compte cependant de la valeur ajoutée que peut représenter le traitement des données (sensibles), les dépenses supplémentaires que doivent faire les unités administratives, industrielles ou commerciales pour assurer la sécurité de leurs données représentent un investissement profitable.
Les autorités judiciaires de leur côté argumentent que le cryptage des données représente un obstacle lors de leurs enquêtes, étant donné que les informations que les autorités sont éventuellement en droit d'intercepter ou d'enregistrer ne peuvent plus être interprétées ou seulement moyennant des efforts considérables. Une solution à ce problème consisterait à déposer les clés auprès d'organes de contrôle afin que ceux-ci soient en mesure le cas échéant d'interpréter les données qu'ils interceptent. Un des arguments est qu'une telle démarche améliorerait la lutte contre le crime. D'autre part, elle entrave le droit de chacun à l'autodétermination en

matière d'information. Nous doutons si un accès aux clés de cryptage permettrait

Veschlüsselungsbild

d'améliorer l'efficacité de la lutte contre le crime. Si les organes de contrôle ont la possibilité de déchiffrer les informations, nous devons nous attendre à ce que les organisations criminelles transmettent leurs informations par le biais d'autres canaux ou qu'ils utilisent - comme ils le font aujourd'hui déjà - des termes qui pour eux ont un autre sens que la signification usuelle. Ceci forcerait de telles organisations à utiliser d'autres procédés ou moyens en plus des possibilités connues pour transmettre leurs informations de manière rapide et sûre. De tels procédés existent aujourd'hui déjà, ainsi il est par exemple possible de remplacer quelques bits d'une image bitmap (par exemple une image d'écran) ou d'un fichier audio par des informations textuelles de telle manière à ce que ces substitutions ne modifient pas la présentation à l'écran ou seulement dans une mesure si minime que les déviations ne soient pas reconnaissables par des non-initiés. Cette technique est connue sous le nom de stéganographie. L'étymologie du mot est grecque, il signifie «signe ou écriture caché». Une autre possibilité pour les autorités judiciaires consisterait à consulter les données au lieu de stockage ou de réception. La gestion des clés devrait dans ce cas être faite de manière à ce que la procédure de déchiffrage devienne transparente.
A notre avis, il est douteux qu'une interdiction de cryptage ou un dépôt de clés auprès d'organes de contrôle améliore l'efficacité de la lutte contre le crime.

6.3. Enregistrement en ligne de logiciels

En prenant comme exemple l'enregistrement en ligne d'un logiciel commercialisé, nous avons examiné plus en détail le traitement des données lié à un tel enregistrement interactif. Notre conclusion est que l'autorisation nécessaire de la part du client n'est pas suffisante.

Certains logiciels commercialisés permettent un enregistrement en ligne comme alternative à l'envoi de la carte d'enregistrement par la poste. Nous avons été rendus attentifs par des tiers au fait que lors d'un tel enregistrement en ligne, des données étaient transférées depuis le PC du client vers l'éditeur du logiciel sans que le client en soit informé ou suffisamment informé.
Il est possible en plus du numéro de série du produit, du nom et de l'adresse du client de transmettre également des informations collectées de manière automatique relatives à la configuration matérielle et logicielle de l'ordinateur du client. Ces données ne sont pas nécessaires pour l'enregistrement du logiciel. L'éditeur les utilise plutôt pour mieux orienter sa stratégie de marketing aux besoins de la clientèle.
Les doutes exprimés quant au fait que l'enregistrement en ligne transmettait plus de données depuis le PC du client que celles qui étaient indiquées n'ont pas pu être vérifiés. Cette possibilité ne peut cependant pas être entièrement exclue.
Le consentement du client présuppose qu'il soit informé *sous une forme qui lui soit compréhensible*, de quelles données sont traitées, de quelle manière et à quelles fins. En ce qui concerne le produit que nous avons testé, la demande de ce consentement était insuffisante. Déjà *avant le premier écran de saisie des données,* les informations suivantes doivent entre autres être communiquées de manière bien visible à l'utilisateur: le but du traitement des données, les données pouvant être saisies ou éventuellement exclues de la transmission, le lieu de stockage, la transmission à l'étranger, des informations relatives au droit d'accès.

L'éditeur en question a accepté nos revendications concernant une meilleure information de l'utilisateur et s'est déclaré prêt à améliorer cet aspect dans un avenir proche.

7. Divers

7.1. Utilisation de données extraites du registre du commerce

Les données figurant dans le registre du commerce sont des données personnelles publiques qu'on ne peut librement utiliser à des fins privées. Le traitement électronique des données permet de combiner rapidement diverses informations qui ne correspondent pas au but initial de leur collecte.

Une personne privée voulait "scanner" les données figurant dans la Feuille officielle suisse du commerce pour communiquer des informations sur demande. Le traitement par un particulier de données personnelles extraites du registre du commerce permettrait de sortir des données officielles du contexte spécifique que constitue le registre officiel et de les exploiter en conséquence. On pourrait à cette occasion répondre aux souhaits de la clientèle et obtenir des informations révélatrices à partir de données relativement simples figurant dans le registre du commerce. Ainsi, grâce aux vastes possibilités de recherche et de sélection qu'offre l'informatique, des données supplémentaires qui n'apparaissent pas directement dans le registre du commerce pourraient être constituées. Le risque de violation de la personnalité des personnes concernées s'en trouverait considérablement augmenté.
C'est le but du registre du commerce qui détermine si des particuliers sont habilités à assembler diverses données personnelles (par ex. nouvelles entreprises, propriétaires d'entreprise ou modifications de statuts). Le fait que le registre ait un caractère officiel ne signifie pas que les données puissent être utilisées sans restriction à des fins privées. Le principe de finalité est également applicable aux données accessibles au public. Ces données ne doivent donc pas être transmises à des tiers à des fins incompatibles avec celles pour lesquelles elles ont été collectées (Principe 2.2 de la Recommandation n° R (91)10 du Comité des ministres du Conseil de l'Europe aux Etats membres pour la transmission à des tiers des données personnelles enregistrées par les organes officiels). Le traitement de données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Si l'exploitation de données du registre du commerce va à l'encontre du principe de finalité, il faudrait, pour qu'elle ne soit pas contraire à la loi, qu'il existe un motif justificatif.
Les personnes concernées doivent avoir la possibilité de faire valoir leur droit d'accès conformément à l'article 8 LPD auprès du maître du fichier. Si la personne concernée demande que ses données soient effacées, cela doit lui être garanti.
Par ailleurs, l'Office du registre du commerce envisage à long terme de permettre au public d'avoir accès aux données du registre du commerce également par le biais d'une banque de données informatique. Les critères régissant la consultation seront élaborés par l'Office du registre du commerce.

7.2. Caractéristiques requises à propos des enveloppes postales (facturation d'honoraires, trafic des paiements)

Quiconque envoie une lettre doit veiller à ce que son contenu demeure confidentiel. La qualité de l'enveloppe ainsi que le format de la fenêtre doivent donc être conçus de telle manière qu'on ne puisse en lire le contenu par transparence ou par la fenêtre.

Une personne privée avait reçu d'un service chargé de l'encaisssement la copie d'une facture d'honoraires dans une enveloppe à fenêtre. Bien que l'enveloppe ait été fermée, la grandeur de la fenêtre permettait de lire diverses données figurant sur la facture. On pouvait notamment y voir combien de temps le patient avait été en traitement auprès du médecin en question, s'il y avait eu changement ou remplacement du médecin, si une incapacité de travail avait été prescrite et si le traitement avait été poursuivi ou interrompu. Ces données constituent des données personnelles. Ce sont en partie des données relatives à la santé, réputées sensibles en vertu de la loi sur la protection des données.
La personne qui traite des donnés personnelles doit en outre veiller à leur confidentialité et en cas de communication ou de transport, empêcher que des tiers non autorisés puissent les lire. Afin de garantir la confidentialité des données concernant les patients lors d'opérations de paiement, il faut utiliser pour l'envoi des factures d'honoraires des enveloppes sans fenêtre, qui ne révèlent aucune information sur les traitements fournis au patient et assurent le secret médical.
Le service de recouvrement concerné a décidé que les copies de factures d'honoraires seront désormais envoyées exclusivement dans des enveloppes fermées sur lesquelles l'adresse sera écrite.
Dans un autre cas, une personne privée s'est plainte de la qualité défectueuse des enveloppes utilisées par des banques. Le papier des enveloppes étant transparent, des tiers non autorisés pouvaient prendre connaissance de ses avis de crédits ou de débits. Le cas a été signalé aux banques en question qui utilisent désormais des enveloppes ne permettant pas de lire les informations concernant les opérations bancaires, donc garantissant le secret bancaire.

IV. ACTIVITES INTERNATIONALES

1. Adhésion à la Convention du Conseil de l'Europe sur la protection des données

Le Conseil fédéral a adopté le 13 novembre 1996 un message à l'attention du Parlement concernant l'adhésion de la Suisse à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (voir FF 1997 I 701); voir également 3e rapport d'activités, p. 193. Cette convention est entrée en vigueur le 1er octobre 1985 et a été, à ce jour, ratifiée par 17 Etats membres du Conseil de l'Europe. L'adhésion pourrait intervenir en 1997, une fois que le Parlement aura adopté l'arrêté fédéral y relatif. L'entrée en vigueur de la Convention interviendrait alors au début 1998.

2. Conseil de l'Europe

Sous présidence suisse, puis sous présidence maltaise, le Groupe de projet sur la protection des données du Conseil de l'Europe s'est réuni à deux reprises. Il a terminé ses travaux en vue de l'adoption d'une recommandation relative à la protection des données médicales. Cette recommandation a été adoptée par le Comité des Ministres lors de sa 584ème réunion, le 13 février 1997. Cette recommandation s'applique à la collecte et au traitement automatisé de données médicales, y compris les données génétiques, tant dans le secteur public que dans le secteur privé, quel que soit le domaine d'utilisation. Elle renforce les obligations de confidentialité notamment en prévoyant que tout traitement de données médicales doit en principe être effectué par des professionnels des soins de santé ou des personnes ou organismes agissant pour le compte de ces professionnels, pour autant que ceux-ci soient soumis à des règles de confidentialité identiques ou comparables. En particulier, elle règle les conditions de licéité de la collecte et du traitement (y. c. le respect des principes de finalité et de proportionnalité) et limite les cas dans lesquels des données médicales peuvent être communiquées. Elle régit les droits des personnes concernées et notamment leur droit à l'information et leur droit d'accès. Elle règle la conservation des données et l'utilisation des données médicales à des fins de recherche scientifique et prévoit l'obligation de prendre des mesures techniques et organisationnelles appropriées contre toute forme de traitement non autorisé. En ce qui concerne les données génétiques, la recommandation s'inspire des dispositions de la Convention pour la protection des droits de l'Homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine (convention bioéthique). Ainsi, en dehors des finalités préventives, diagnostiques, thérapeutiques, de recherche scientifique et des besoins d'une procédure judiciaire ou d'une enquête pénale régis par une loi prévoyant des garanties appropriées, le traitement des données génétiques n'est permis que pour des raisons de santé. Cela exclut en particulier la collecte et le traitement de données génétiques à des fins prédictives non liées à des raisons de santé, sauf existence d'un intérêt supérieur.

Le Groupe de projet sur la protection des données a également pratiquement terminé ses travaux en vue de l'adoption d'une recommandation relative à la protection des données à caractère personnel collectées et traitées à des fins statistiques. Le texte proposé renforce la protection et la confidentialité des données collectées et traitées à des fins statistiques tout en reconnaissant les besoins des statisticiens de recourir relativement aisément à la collecte et au traitement de données personnelles. Ce document est le fruit d'une franche et constructive collaboration entre des experts en protection des données et des statisticiens, et notamment entre le PFPD et l'Office fédéral de la statistique. Cette recommandation, vraisemblablement adoptée par le Comité des Ministres cette année encore, régit la collecte et le traitement des données à des fins statistiques dans les secteurs public et privé. Elle fixe les conditions de licéité de la collecte et du traitement des données à des fins statistiques et prévoit notamment des exigences strictes quant à la confidentialité et au respect des principes de proportionnalité et de finalité. Ainsi, les données collectées et traitées à des fins statistiques doivent servir uniquement à ces fins. Elles ne doivent pas être utilisées pour prendre une décision ou mesure relative à la personne concernée. La recommandation attache également une grande importance à la transparence des traitements et notamment à l'information des personnes concernées.

Le Groupe de projet a par ailleurs entamé l'examen d'un projet de recommandation dans le domaine des assurances élaboré par le groupe de travail 14 auquel nous avons également activement participé.
Enfin, le groupe de travail 15 sur les nouvelles technologies de l'information a poursuivi ses travaux. Il devrait consacrer ses efforts en particulier sur les inforoutes, les cartes à puce, la surveillance électronique (notamment vidéosurveillance) et la gestion des ressources d'information.
Le comité consultatif mis en place par la Convention 108 et qui est chargé en particulier de donner des avis sur l'application de ladite Convention a tenu sa 12e réunion. Il s'est en particulier penché sur la pertinence des définitions et principes de la Convention eu égard aux développements technologiques actuels.

3. Conférence Internationale des Commissaires à la protection des données

La XVIIIe Conférence Internationale des Commissaires à la protection des données s'est déroulée à Ottawa (CAN) du 18 au 20 septembre 1996 à l'invitation du commissaire canadien. La Conférence réunissait les commissaires à la protection des données de 23 Etats, des experts gouvernementaux, des représentants de l'Union européenne, ainsi que de l'industrie de l'information, de l'économie, de la science et des services. La Suisse y était représentée par le préposé fédéral et par le préposé du canton de Zurich. La Conférence a permis un échange d'informations sur les développements récents en matière de protection des données et notamment les problèmes soulevés par la directive européenne dans l'échange d'informations personnelles entre les pays de l'Union européenne et les pays tiers. Placée sous le thème «la Vie privée au-delà des frontières», la conférence s'est penchée sur les conséquences de l'accroissement du commerce international de renseignements et de données pour le respect des droits et libertés fondamentaux, notamment de la vie privée des personnes. Les garanties de la protection des données deviennent plus que jamais primordiales face au recours incontournable aux services électroniques et aux réseaux d'information (inforoute) par les administrations publiques, les entreprises privées et les particuliers. Face à cette évolution vers «le village global», il apparaît nécessaire de renforcer l'information des citoyens-consommateurs, de développer des codes de conduite en matière de protection des données, ainsi que de nouvelles solutions juridiques et techniques. Il est en particulier important de concevoir de tels instruments pour combler le déficit en protection des données lors d'échanges d'informations entre des Etats régis par des législations de protection des données et des Etats sans protection adéquate, tels par exemple les Etats-Unis. Sans une véritable prise de conscience à tous les niveaux, cette évolution pourrait entraîner la fin de la vie privée. La Conférence a permis d'illustrer cette évolution par de nombreux exemples. Citons notamment l'utilisation des cartes de crédits, la création de mégabanques de données par le recours à Internet, les flux trans-frontières entre l'Europe et les Etats-Unis, les systèmes de réservation, tel Galileo ou Amadeus, les multimédias tels la télévision interactive et le E-Mail (problème de l'anonymat et de la confidentialité). L'identification des personnes (p. ex. lors de l'utilisation des cartes de crédit), le traitement de données de santé, l'expansion des cartes de santé, les données génétiques et la surveillance des drogués ont également été évoqués. La nécessité de limiter le traitement des données

PC-Einbrecher

personnelles et de renforcer les mesures d'éthique et de confidentialité des données médicales a finalement été soulignée.

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

L'objectif visé par le groupe de travail cité ci-dessus consiste à améliorer la protection des données dans le domaine des télécommunications et des médias. La 20ème séance du groupe de travail a eu lieu les 18 et 19 novembre 1996 à Berlin sous la présidence du Préposé à la protection des données de Berlin.
Le mémorandum concernant la protection des données et la vie privée sur Internet, déjà discuté lors de séances précédentes, a été revu et accepté. Vous en trouverez le texte à la page 214 de ce rapport. En outre, les thèmes suivants ont entre autres été discutés lors d'exposés et de séances de discussion: les systèmes permettant de coter et de filtrer certaines offres sur Internet, l'accès à des données médicales à travers Internet, la question du cryptage des données, les méthodes de paiement électronique (Electronic Cash), les systèmes internationaux de transport et de réservation ainsi que la coopération future du groupe de travail avec d'autres comités.
Dans le domaine des télécommunications, seules des solutions transfrontières sont appropriées. C'est pourquoi la coopération au niveau international entre les organes de protection des données revêt une importance primordiale.

5. Accords bilatéraux et multilatéraux sur la réadmission et le transit d'anciens réfugiés de guerre

Avec le retour espéré à la normalité se pose aussi la question du rapatriement et du transit par territoire étranger d'anciens réfugiés de guerre vers leur pays d'origine. Les accords respectifs que la Suisse et d'autres pays ont conclus avec la Croatie et la Yougoslavie règlent également l'aspect de la protection des données. On peut cependant se demander si ces dispositions sont appliquées correctement par les factions guerrières d'autrefois et si leur transposition est surveillée.

En ce qui concerne la Croatie, on nous a soumis trois accords pour prise de position, à savoir un accord (bilatéral) sur le *rapatriement* ainsi qu'un accord bilatéral et un accord multilatéral sur le *transit* de personnes à travers la Croatie. L'accord de rapatriement constitue un complément (protocole) à un accord du 8/9 février 1993 (RS 0.142.112.912) et ne règle pas ou pas suffisamment les aspects de protection des données. Nous avons demandé un amendement le rendant conforme aux normes suisses et européennes. On nous a promis ce dernier pour une date ultérieure, au plus tard dans deux ans. Les deux accords de transit règlent la protection des données conformément aux normes suisses et européennes. Compte tenu de la situation réelle, nous avons posé la question de savoir si ces dispositions de protection des données étaient vraiment appliquées et si certains mécanismes de contrôle minimaux étaient prévus (par ex. dans le cadre de l'accord de Dayton). Il est donc absolument nécessaire de prendre des mesures appropriées en attendant que la situation redevienne complètement normale. A notre avis, les données

personnelles visibles sur les visas à présenter doivent être restreintes (par ex. en supprimant de manière stricte les indications concernant l'appartenance à une ethnie, etc.).
On peut qualifier d'encourageant le fait que la Croatie vient également de se donner une loi sur la protection des données. Par contre, la République fédérale de Yougoslavie ne connaît actuellement pas de loi sur la protection des données. Même si l'accord de rapatriement et de réadmission qui nous a également été soumis est conforme aux normes suisses et européennes, les questions de l'application de ces normes de protection de données et de contrôle se posent néanmoins.

6. L'intégration d'une clause de protection des données dans la convention quadripartite (A, CH, D, FL) concernant la sécurité sociale

L'Allemagne a demandé l'intégration d'une clause de protection des données dans la deuxième convention complémentaire relative à la Convention quadripartite concernant la sécurité sociale. Nous saluons cette proposition car elle correspond sur le fond en substance à la LPD ainsi qu'aux normes minimales reconnues au niveau international en ce qui concerne la protection des données.

En décembre 1996, des discussions ont eu lieu à Berne entre des représentants de l'Allemagne, du Liechtenstein, de l'Autriche et de la Suisse à propos de l'intégration d'une clause de protection des données dans la convention mentionnée. Dans le cadre de ces discussions, nous avons été priés par la délégation suisse (Office fédéral des assurances sociales) de prendre position.
Nous avons jugé positive la clause de protection des données proposée par l'Allemagne. Cela surtout parce qu'elle rend les principes de protection des données figurant dans la clause (finalité, proportionnalité, droit d'accès, etc,) transparents pour les autorités comme pour les personnes concernées. D'une part cette clause servira de guide aux autorités, d'autre part les citoyens concernés par cette convention seront désormais suffisamment informés du traitement de données les concernant.
En outre, la clause de protection des données contient en susbtance les normes minimales applicables à l'échelle internationale et n'implique rien de nouveau pour la Suisse, autrement dit elle est pratiquement identique à la loi suisse sur la protection des données. Elle n'implique donc pas pour les autorités suisses de modification matérielle pour ce qui est du traitement des données, d'autant plus qu'elle n'est appliquée que lorsque le droit national ne prévoit pas de réglement (caractère subsidiaire de la clause).
Les délégations du Liechtenstein, de l'Autriche et de la Suisse examinent actuellement de nouveau la proposition de l'Allemagne. On ne sait encore quand et dans quelle mesure la clause de protection des données sera intégrée à la convention.

V. REGISTRE DES FICHIERS (DATAREG)

1. Système de gestion du registre des fichiers

En service depuis plus de deux ans maintenant, le système de gestion du registre des fichiers permet, à partir des saisies effectuées, de tirer des conclusions sur l'impact et les propriétés des déclarations de fichiers.

Alors que l'année 1994 a été placée sous le signe de la mise en service officielle de DATAREG et 1995 de son optimisation, l'année 1996 a enfin permis de disposer d'un système entièrement opérationnel.
Afin de donner cette année aussi une image des propriétés et de l'impact des déclarations de fichiers, il a été procédé à un certain nombre de relevés concernant DATAREG. Les considérations et chiffres ci-dessous relatifs aux fichiers enregistrés se rapportent à l'état du registre en janvier 1997.
1480 fichiers au total ont été enregistrés, dont 33 ont déjà été effacés sur demande du maître du fichier. 1143 fichiers émanent d'organes fédéraux et 337 de particuliers. Sur les 1480 fichiers enregistrés, tous sont soumis à publication à l'exception de 38 d'entre eux.
1209 catégories de données personnelles traitées ont été jusqu'ici enregistrées pour les différents fichiers. Ces catégories ont été utilisées 9128 fois. Donc, en moyenne, 6 catégories de données personnelles ont été annoncées par fichier. Les catégories de données personnelles les plus souvent mentionnées sont l'adresse, la profession, l'identité, la nationalité/le lieu d'origine, le lieu de travail et les langues, puis le numéro AVS, la formation, la famille, la santé et le revenu.
862 catégories de destinataires de données et de participants ont été enregistrées. Elles ont été citées 2616 fois comme destinataires et 636 fois comme participants.
En ce qui concerne les déclarations faites par les organes fédéraux, 504 bases juridiques différentes ont été jusqu'ici mentionnées. Elles ont été utilisées 1330 fois.
1227 adresses de maîtres de fichiers ont été jusqu'ici intégrées dans le système. 55 catégories de branches ont été attribuées pour la saisie de fichiers privés.

2. Publication du registre des fichiers

Le registre des fichiers a été publié en 1996, pour la première fois depuis l'entrée en vigueur de la loi sur la protection des données. La publication des fichiers de personnes privées a fait l'objet d'un volume, réparti en 33 branches. La publication des organes fédéraux a été scindée en trois volumes. Les registres sont disponibles auprès de l'Office fédéral des imprimés et du matériel.

Le registre des fichiers a été publié pour la première fois en 1996 (état 31 mars 1996) et présenté à l'occasion de la conférence de presse du PFPD. Cette publication a été précédée de travaux portant sur la forme, le contenu et la composition du registre. Il s'est très vite avéré de l'avis de tous qu'une publication séparée pour les organes fédéraux et pour les personnes privées s'imposait.
Le contenu du fichier comprend pour les organes fédéraux: la désignation et le numéro de registre du fichier, le cercle des personnes concernées, leur nombre approximatif, le but du fichier, la base juridique, le maître du fichier, l'organe auprès duquel peut être exercé le droit d'accès, les catégories de données personnelles

traitées, les catégories de destinataires des données ainsi que les catégories de participants.
Le contenu du fichier comprend pour les personnes privées: la désignation et le numéro de registre du fichier, le but du fichier, le maître du fichier, la personne auprès de laquelle peut être exercé le droit d'accès, les catégories de données personnelles traitées, les catégories de destinataires des données ainsi que les catégories de participants.
Un volume rassemble tous les fichiers déclarés par les personnes privées (volume B1). Ce volume contient 337 fichiers répartis en 33 branches. Les branches sont classées par ordre alphabétique et à l'intérieur des branches, les fichiers sont structurés d'après les maîtres des fichiers, également par ordre alphabétique.
Trois volumes rassemblent les fichiers déclarés par les organes fédéraux. Le volume A1 renferme les fichiers du Département fédéral de l'intérieur, A2 les fichiers du Département fédéral des finances et de la Banque nationale, et A3 ceux des assurances sociales.
Ces fichiers ont fait l'objet d'environ 600 déclarations ordinaires et quelque 150 déclarations simplifiées. Les fichiers sont classés par département et à l'intérieur des départements, par déclarations ordinaires et simplifiées, ainsi que par offices. Les volumes A4 et A5 (état 28 février 1997) concernant également des organes fédéraux sont quant à eux publiés en même temps que le présent rapport.
Le volume A4 contient les fichiers de la Chancellerie fédérale, de l'Assemblée fédérale, du Département fédéral des affaires étrangères et du Département fédéral de justice et police (à l'exception de l'Office fédéral de la police).
Le volume A5 contient les fichiers du Département fédéral de l'économie publique, du Département fédéral des transports, des communications et de l'énergie (à l'exception des PTT et de l'Office fédéral de la communication), de l'Office fédéral de l'informatique, du Tribunal fédéral et du Tribunal fédéral des assurances.

VI. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

1. Fonctionnement du secrétariat

L'année écoulée a été pour nous une année exceptionnelle. L'ampleur rapide prise par le traitement électronique des données dans les domaines privé et public, y compris le phénomène d'imbrication de différents systèmes de traitement, nous a incité à réfléchir sur la manière d'assurer nos tâches à l'avenir. En outre, de nouveaux locaux en dehors de Berne ont été attribués à notre secrétariat. Etant donné que nos activités nécessitent une mobilité accrue de la part des collaborateurs du secrétariat (fonction de conseil et de contrôle), le déménagement à Zollikofen s'est traduit par une perte considérable d'heures de travail et de qualité du travail. Nos tâches n'en ont été que plus difficiles à accomplir. Nombre de sociétés ou de personnes privées qui nous avaient priés de leur accorder une entrevue se sont ensuite plaintes de l'éloignement de l'endroit et de la mauvaise qualité des liaisons assurées par les transports publics.
Trois collaborateurs ont quitté le secrétariat au cours de l'année écoulée et ont été remplacés. Par ailleurs, la création d'un nouveau poste a été autorisée pour renforcer l'équipe du Secrétariat, notamment dans le domaine des assurances sociales.

2. Evolution des tâches

Le nombre des demandes qui nous ont été transmises cette année a considérablement augmenté. A nouveau, les questions d'ordre juridique concernaient essentiellement les affaires de police, le droit des étrangers, les assurances et la santé. L'administration fédérale a transmis davantage de demandes sur l'imbrication des systèmes de traitement de données et sur la transmission de données personnelles à des tiers. Les personnes privées ont au total davantage fait usage de la possibilité de demander conseil. Les principaux thèmes abordés dans les demandes sont l'exercice du droit d'accès et les possibilités de rectification et d'effacement des données figurant dans des fichiers gérés par des personnes privées.

3. Information du public

Nous avons avant tout cherché à familiariser les citoyens avec les dispositions légales de protection des données. Nous avons ainsi participé à diverses conférences et réunions d'information. Nous avons également envoyé bon nombre de brochures. Celles-ci ont rencontré un large écho auprès de la population. A ce propos, nous ne pouvons nous permettre des tirages très élevés pour des raisons d'économie. Ne disposant pas d'un budget propre, nous ne sommes pas en mesure de faire réimprimer un nombre suffisant de brochures. Nous sommes donc souvent obligés de n'envoyer que des copies.
Entre-temps, nous avons également publié la brochure relative au traitement de données personnelles dans le domaine médical.
Par ailleurs, nous sommes également présents sur Internet avec une offre propre qui permet donc aussi d'appeler par le réseau des informations sur la protection des données.
Aux pages 202ss , nous avons représenté graphiquement sous forme de tableau un choix des diverses demandes téléphoniques qui nous sont parvenues.

Le PFPD sur Internet

Du point de vue de la protection des données, Internet incite à de nombreuses prises de position bien critiques (voir le mémorandum Budapest-Berlin, page 214). Internet est néanmoins un support excellent pour la diffusion actuelle et sans grands frais de nos publications.

Afin de rendre nos informations accessibles au public intéressé de manière rapide et efficace, nous nous sommes décidés à utiliser Internet comme moyen d'information supplémentaire. La majorité de nos publications (guides, rapports, recommandations, communiqués de presse) sont disponibles sur Internet. Même le texte de la loi sur la protection des données avec ses ordonnances ainsi que les dispositions internationales en matière de protection des données peuvent être consultés. Nous offrons en outre aussi des liens vers d'autres pages Internet qui s'occupent de protection et de sécurité des données. Nous mettons également à disposition un outil de recherche permettant de rechercher l'ensemble des documents que nous proposons selon des mots-clés.

Internetbild

4. Troisième conférence Suisse des délégués à la protection des données (1996)

Les deux premières conférences suisses sur la protection des données en 1993 et 1995 ayant été organisées par le Préposé fédéral à la protection des données, l'hôte de la conférence de 1996 fut pour la première fois un canton, plus précisément le préposé à la protection des données du canton de Zurich.
Les sujets suivants ont entre autres été abordés: l'utilisation des données du recensement de la population à des fins administratives, la protection des données pour les dossiers d'identification judiciaire de la police ainsi que lors de l'archivage.
Finalement la conférence, suivie par de nombreux représentants des cantons, adopta une résolution demandant à tous les acteurs de la santé publique d'attacher plus d'importance à la protection des données.
Le 3 octobre 1996, le préposé à la protection des données du canton de Zurich organisa en collaboration avec l'EPFZ un symposium très suivi de *protection et de sécurité des données* sur le thème «Les technologies de l'information en réseau et la protection des données».

5. Statistique des activités du PFPD Période du 1er avril 1996 au 31 mars 1997

Période du 1er avril 1996 au 31 mars 1997

Participations à des conférences:

Nationales	Internationales
19	15

Nombre de séances:

	Confédération	Personnes privées	Cantons
A l'intérieur	98	32	0
A l'extérieur	285	32	16
Total	383	64	16

Nombre de prises de position

Nombre de prises de position

Renseignements par telephone

Renseignements par téléphone
Selon la provenance des appels

Renseignements par téléphone
Par matière

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

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

VII. ANNEXES

1. Feuille d'information: Blocage d'une adresse utilisée à des fins publicitaires

Blocage d'une adresse utilisée à des fins publicitaires

En vertu de la loi fédérale sur la protection des données, l'utilisation d'une adresse à des fins publicitaires est en principe autorisée si la personne concernée:
1. a rendu son adresse accessible au public et
2. n'en a pas interdit l'utilisation à des fins publicitaires.

1. L'adresse est par exemple **accessible au public**, lorsque
- elle figure dans l'annuaire téléphonique,
- elle apparaît dans d'autres répertoires (annuaire par branches d'activités, catalogue d'adresses édité par une association ou une société privée, etc.).

2. **L'utilisation de l'adresse à des fins publicitaires** peut faire l'objet

*d'une **interdiction** générale*:

- En demandant aux Télécom (PTT) que l'adresse soit bloquée. Dans l'annuaire téléphonique, elle sera marquée d'un *. Les formules de demande requises se trouvent dans tous les annuaires.
- En demandant à l'Association suisse pour le marketing direct, à laquelle est rattachée la majorité des sociétés suisses de marketing direct, que l'adresse soit bloquée.

  Adresse: Association suisse pour le marketing direct, case postale, 8708 Männedorf

*d'une **interdiction** au cas par cas:*

- En renvoyant à l'expéditeur les textes publicitaires que l'on ne souhaite pas recevoir, avec la mention „J'interdis l'utilisation de mon adresse à des fins publicitaires." (afin de disposer d'une preuve, mieux vaut effectuer le renvoi en recommandé).
- En ajoutant ladite mention à chaque communication de l'adresse personnelle (concours, demandes d'informations, adhésions à des associations, dons, commandes auprès de maisons de V.P.C., cartes de client, cartes de rabais, etc.).

Le commerce d'adresses à des fins publicitaires étant florissant en Suisse, tout comme dans d'autres pays d'ailleurs, il est difficile de se prémunir complètement contre l'envoi de publicité. Toutefois, le recours systématique aux possibilités susmentionnées de bloquer son adresse entraîne en tout cas une forte réduction de ce genre d'envois.

En vertu de la loi sur la protection des données, chacun a le droit de demander au maître d'un fichier si des **informations** le concernant sont traitées et, le cas échéant, quel est le genre de ces informations. Le *Guide du préposé fédéral à la protection des données sur les droits de la personne concernée* renseigne dans le détail au sujet du droit d'accès à ses données personnelles.

Pour commander le guide et demander des renseignements supplémentaires s'adresser au *préposé fédéral à la protection des données , 3003 Berne, tél.: 031/322 43 95*.

2. Directives de l'Office fédéral du personnel régissant les conditions d'utilisation des tests individuels et collectifs dans l'administration générale de la Confédération.

(du 6 novembre 1996)

1. But des tests individuels et collectifs

Les tests individuels et collectifs psychométriques (comme les tests de performance, d'intelligence ou de la personnalité) et d'autres méthodes d'évaluation de la personnalité ou des performances (telles que les expertises graphologiques, les notices biographiques, assessment, assessment-center) servent à évaluer de façon systématique les capacités du personnel en fonction ou des futurs collaborateurs ainsi que leurs potentialités professionnelles ou personnelles.

2. Principes régissant l'utilisation des tests individuels et collectifs dans l'administration générale de la Confédération

2.1. Il ne doit être fait usage du test individuel ou du test collectif que si:

- les informations requises pour l'appréciation sont insuffisantes,
- les personnes à évaluer occupent ou sont appelées à occuper des fonctions supérieures,
- il y a lieu de repourvoir un poste clé,
- le test peut être utilisé pour un grand nombre de personnes lors de procédures de promotion ou de sélection périodiques

et si cela se justifie au regard du coût et de la rentabilité.

2.2. L'emploi de tests psychométriques et d'autres méthodes d'évaluation dans le cadre des procédures d'avancement et de sélection du personnel dans l'administration générale de la Confédération est du ressort des départements et des offices fédéraux. Ils répondent entièrement du choix, du financement et de l'utilisation des tests. En s'inspirant des présentes directives, les départements déterminent par voie de règlement interne les tests applicables selon les besoins spécifiques de leurs services. Les offices (directions) désignent les personnes chargées de faire passer les tests. Ils veilleront à ce qu'elles acquièrent les connaissances requises en la matière et qu'elles soient assistées sur le plan pratique par des psychologues professionnels (disposant d'une formation reconnue de la FSP[1)] ou d'un diplôme de l'IPA[2)]), capables de conduire un test, d'en dépouiller les résultats et de les interpréter (le vendeur du test peut également proposer les services de ses spécialistes dont les qualifications doivent être comparables à celles des psychologues).

2.3. Le respect des présentes directives garantit un déroulement loyal et honnête du test et le respect de la législation sur la protection des données.

2.4. Le Département fédéral des affaires étrangères édicte conformément aux présentes directives et d'entente avec l'Office fédéral du personnel des

directives internes régissant la procédure d'admission au service diplomatique et consulaire.

3. Règles d'application

3.1. Seuls sont autorisés les tests **scientifiquement reconnus** et **conduits selon des principes professionnels.**

3.2. Avant de faire passer les tests, il convient de déterminer précisément les exigences requises et de les pondérer. On en tirera ensuite les critères de sélection ou d'avancement applicables aux postes existants et futurs. Les résultats des tests doivent corréler avec les critères et apporter les réponses attendues.

3.3. Le nombre et l'étendue des tests réalisés (y compris l'évaluation des données déjà disponibles) de même que la qualité des résultats escomptés sont déterminés en fonction de l'importance du poste ou de l'avancement prévu. L'investissement en personnel, en temps et les dépenses doivent être évalués rigoureusement.

3.4. **Le test psychométrique ou quel que soit le procédé retenu ne peut être utilisé comme unique ou principal instrument d'évaluation.** En d'autres termes l'utilisation du test individuel ou du test collectif ne dispense pas de l'obligation d'examiner le dossier de postulation ou les prestations déjà connues ni de procéder à un entretien individuel d'évaluation, de sélection ou d'avancement ni de décider du choix du candidat ou d'un avancement.

3.5. Les tests doivent être proposés dans les trois langues officielles (allemand, français et italien).

4. Protection de la personnalité

4.1. Avant de soumettre une personne à un test, il y a lieu de requérir son **assentiment**.

4.2. Toute **discrétion** doit être assurée. Lorsque deux ou plusieurs personnes d'un même office ou d'une même entreprise se soumettent à un test et que l'anonymat ne peut être garanti (p. ex. dans le cadre d'un assessment-center), lesdites personnes en seront informées préalablement.

4.3. La personne soumise à un test a le droit de consulter en tout temps et sans restriction les pièces relatives au test (telles que les questionnaires, les barèmes d'évaluation, les analyses de l'ordinateur) ainsi que toutes les données afférentes (comme les réponses rendues lors du test, les résultats du test, les évaluations globales).

4.4. Les résultats des tests **ne sont pas des données objectives**. Les données collectées de même que leur mode d'évaluation sont le reflet de la vision de l'homme ou de la personnalité qui sous-tend les tests. La personne soumise à un test doit donc être autorisée **en tout temps à exprimer son avis** sur les résultats du test et leur interprétation.

5. Utilisation des résultats du test

5.1. La personne soumise à un test doit être informée préalablement sur le but du test et sur l'usage qui sera fait des résultats. Le test et les données afférentes ne peuvent être affectés **à d'autre but que celui convenu avec la personne soumise au test**.

5.2. Les données doivent être protégées par des mesures techniques et organisationnelles appropriées **contre tout accès et utilisation non autorisés.**

En principe, seules sont habilitées à consulter les réponses et les résultats la personne ayant subi le test et celle qui l'a fait passer. Le cas échéant, l'autorité qui décide ne peut avoir accès qu'à une **appréciation globale** des résultats.

5.3. Les données afférentes à un test de sélection sont conservées jusqu'au terme de la procédure; tous les originaux sans exception sont remis à la personne ayant subi le test une fois la procédure close.

Les pièces afférentes aux tests, les résultats ou les appréciations globales destinés à des évaluations internes et qui sont utilisés par la suite peuvent être conservés sous clé dans le dossier du personnel. Les résultats des tests ne reflètent cependant qu'une image temporaire des capacités des personnes qui s'y sont soumises. Il y aura donc lieu de réexaminer la validité de ces résultats après deux ans au plus avec la personne ayant subi le test (p. ex. à la faveur des entretiens portant sur l'appréciation du personnel) et de relever le résultat de cet examen (p. ex. dans une note qui figurera dans le dossier d'appréciation).

On ne conservera aucune donnée concernant les personnes qui n'ont pas été engagées.

5.4. Les données relatives aux tests ne peuvent être utilisées à des **fins statistiques**, tant par les concepteurs que par les vendeurs des tests, qu'avec l'assentiment de la personne ayant subi le test et après avoir été épurées des éléments susceptibles de l'identifier.

5.5. Au demeurant, on observera la circulaire de l'OFPER du 26.01.1984 concernant la protection des données relatives au personnel dans l'administration générale de la Confédération (C.3028). Sont applicables en outre les articles 8 ss de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD) et les publications afférentes du Préposé fédéral à la protection des données notamment le "Guide pour le traitement des données personnelles dans l'administration fédérale" 1994.

3. La protection des données sur Internet - «Budapest - Berlin Memorandum»

Le document est une traduction de l'originial anglais «Data Protection and Privacy on the Internet, Raport and Guidance» par le Conseil d'Europe.

La protection des données et le secret sur Internet
Rapport et lignes directrices

(adoptés lors de la 20e réunion du Groupe de travail international sur la protection des données dans les Télécommunications
à Berlin
le 19 novembre 1996
sur la base des discussions de la 19e réunion du Groupe à Budapest
les 15 et 16 avril 1996)

Résumé

Il ne fait aucun doute que la protection juridique et technique de la vie privée des utilisateurs d'Internet est actuellement insuffisante.

Dix principes directeurs sont définis dans le présent document pour améliorer la protection de la vie privée sur le Net:

1. Les prestataires de services devraient informer de façon non équivoque chaque utilisateur du Net des risques concernant le secret de la vie privée. Ce sera alors à l'utilisateur de peser ces risques en fonction des avantages escomptés.

2. Dans bien des cas, la décision de se brancher sur Internet et la façon de l'utiliser sont soumises à des conditions juridiques dans le cadre de la législation nationale sur la protection des données.
Cela signifie, par exemple, que les données personnelles ne peuvent être collectées que de façon transparente. Les données concernant les "patients" et les autres données sensibles ne devraient être transmises par l'intermédiaire d'Internet ou stockées sur des ordinateurs reliés au Net que si elles sont cryptées. Les avis de recherche émis par la police ne doivent pas être publiés sur Internet.

3. Les initiatives visant à mettre sur pied une coopération internationale plus étroite ou même une convention internationale régissant la protection des données dans le contexte des réseaux et services transfrontières doivent être soutenues.

4. Il est nécessaire de créer un mécanisme de surveillance international qui pourrait s'appuyer sur les structures existantes telles que l'Internet Society et d'autres organismes. La responsabilité de la protection de la vie privée devra être institutionnalisée dans une certaine mesure.

5. La législation nationale et internationale doit stipuler de façon non équivoque que le processus de communication (par exemple par courrier électronique) est également protégé par le secret des télécommunications et de la correspondance.

6. En outre, il est nécessaire d'élaborer des moyens techniques pour améliorer le secret de la vie privée de l'utilisateur sur le Net. Il est indispensable d'élaborer des principes de conception pour la technologie de l'information et des communications et pour le matériel et le logiciel multimédias permettant à l'utilisateur individuel de contrôler l'utilisation de ses données personnelles et d'en obtenir communication en retour. D'une manière générale, les utilisateurs doivent avoir la possibilité d'accéder à Internet sans devoir révéler leur identité, lorsque les données personnelles ne sont pas nécessaires à la prestation d'un service déterminé.

7. Des moyens techniques doivent aussi être mis en œuvre en vue de protéger la confidentialité. En particulier l'utilisation de méthodes sûres de cryptage doit devenir et rester une option légitime pour tout utilisateur d'Internet.

8. Le Groupe de travail soutiendrait une étude de faisabilité concernant la mise au point d'une nouvelle méthode de certification délivrant des "labels de qualité" aux fournisseurs et aux produits pour leur aptitude à la protection du secret de la vie privée. Cela pourrait aboutir à améliorer la transparence pour les utilisateurs des autoroutes de l'information.

9. L'anonymat est un élément complémentaire essentiel à la protection de la vie privée sur Internet. Les limitations du principe de l'anonymat doivent être strictement limitées à ce qui est nécessaire dans une société démocratique, sans remettre en question le principe en lui-même.

10. Enfin, un élément décisif consistera à étudier comment une autorégulation reposant sur une "Netiquette" étendue et une technologie favorable au secret de la vie privée sont susceptibles d'améliorer la mise en œuvre des réglementations nationales et internationales sur la protection de la vie privée. Il ne suffira pas de s'en remettre à un seul de ces modes d'action: ils devront être combinés de façon efficace pour parvenir à une infrastructure d'information mondiale respectant les droits de l'Homme au secret de la vie privée et à des communications non surveillées.

Rapport

Internet est aujourd'hui le plus grand réseau informatique international du monde. Il y a des "bretelles d'accès" à cette "autoroute de l'information" dans plus de 140 pays. Internet est constitué de plus de quatre millions de sites Internet ("hôtes"); plus de 40 millions d'utilisateurs répartis dans le monde entier peuvent utiliser au moins un des différents services Internet et peuvent ainsi communiquer les uns avec les autres par courrier électronique. Les utilisateurs ont accès à un immense gisement d'informations stockées en divers endroits sur toute la terre. Internet peut être considéré comme le premier niveau d'une infrastructure d'information mondiale émergeante. Le WorlWideWeb (WWW), considéré comme l'interface la plus moderne pour les utilisateurs d'Internet, sert de base à de nouveaux services multimédias interactifs. Les protocoles Internet sont de plus en plus utilisés pour les communications à l'intérieur des grandes entreprises ("Intranets").

Les participants à Internet ont des tâches, des possibilités et des intérêts divers:

* Les entreprises de logiciel, de matériel informatique et de télécommunications conçoivent les réseaux et les services mis à la disposition du public.

* Les organismes de télécommunications comme les Télécom nationales fournissent les réseaux de base pour le transfert des données (connexions point à point ou point-à-multipoint).

* Les fournisseurs d'accès (communications) fournissent les services de base pour le stockage, la transmission et la présentation des données. Ils sont responsables du système de transport d'Internet (acheminement et livraison) et ils traitent les données de trafic.

* Les fournisseurs d'information (contenu) fournissent aux usagers les informations stockées dans des fichiers et des bases de données.

* Les utilisateurs accèdent aux divers types de services Internet (messagerie, journaux, information) et utilisent le Net à des fins ludiques aussi bien que pour le télé-achat, le télétravail, le télé-enseignement/apprentissage et la télémédecine.

1. Problèmes et risques

Contrairement au traitement traditionnel des données personnelles, dans lequel une seule autorité ou entreprise est responsable de la protection de la vie privée de ses clients, ce type de responsabilité globale incombant à une entité déterminée n'existe pas sur Internet. En outre, il n'y a pas de mécanisme international de surveillance chargé de faire appliquer les obligations légales dans la mesure où celles-ci existent. L'utilisateur est donc obligé de faire confiance à la sécurité de l'ensemble du réseau et, par conséquent, de chaque élément de celui-ci, où qu'il se trouve et quel qu'en soit le gestionnaire. La confiance que l'on peut accorder au Net va devenir un élément encore plus crucial avec l'arrivée de nouveaux logiciels qui, non seulement poussent l'utilisateur à télécharger des programmes à partir du Net, mais affaiblissent aussi le contrôle qu'il peut exercer sur ses données personnelles.
La croissance rapide d'Internet et son utilisation de plus en plus fréquente à des fins commerciales et privées soulève de graves problèmes de respect de la vie privée:

* Internet facilite la transmission rapide de grandes quantités d'informations à destination de tout système informatique relié au réseau. Les données sensibles peuvent être communiquées à des pays ne disposant pas du niveau de protection des données approprié. Les fournisseurs d'informations peuvent offrir des données personnelles à partir de sites situés dans des pays dépourvus de toute législation sur la protection de la vie privée et où l'on peut accéder à ces données à partir de n'importe quel point du monde, d'un simple clic de souris.

* Les données personnelles peuvent être acheminées en passant par des pays sans aucune législation de protection des données ou avec une législation insuffisante. Sur Internet, conçu à la base à des fins universitaires, la confidentialité des communications n'est pas assurée.

  Il n'y a ni commutation centralisée, ni aucune autre autorité responsable exerçant son contrôle sur l'ensemble du réseau. La responsabilité de la protection des données et de leur confidentialité est donc partagée entre des

millions de prestataires. Tout message transmis peut être intercepté au niveau de chaque site où il passe et peut être suivi, modifié, contrefait, supprimé ou retardé. Néanmoins, l'utilisation d'Internet à des fins commerciales augmente de façon exponentielle et les données personnelles ou autres données sensibles (données de carte de crédit aussi bien qu'informations médicales individuelles) sont transmises par Internet.

* L'utilisation des services Internet ne permet pas un anonymat convenable ni une authentification adéquate. Les protocoles de réseaux informatiques et beaucoup de services Internet travaillent généralement en communication point-à-point. Outre les données à transmettre, l'identification (ID) de l'expéditeur et du destinataire est également transmise. Chaque message de messagerie électronique contient un en-tête portant des renseignements sur l'expéditeur et le destinataire (nom et adresse IP, nom de l'ordinateur hôte, heure d'expédition). L'en-tête contient, en outre, des renseignements sur l'acheminement et le sujet du message. Il peut également contenir des références aux articles d'autres auteurs. Les utilisateurs sont obligés de laisser une trace électronique qui peut être utilisée pour établir le profil de ses intérêts et de ses goûts personnels. Bien qu'il n'existe pas de comptabilité centralisée des accès aux informations ou au WorlWideWeb, le comportement informationnel des expéditeurs et des destinataires peut être reconstitué et surveillé, au moins par le fournisseur d'accès auquel l'utilisateur est connecté. D'autre part, la faiblesse des procédures d'identification et d'authentification sur Internet a été mise à profit pour pénétrer dans des systèmes informatiques distants qui étaient insuffisamment protégés, afin d'espionner les informations qui y étaient enregistrées, de les manipuler ou de les effacer. L'absence d'authentification sûre pourrait aussi être utilisée pour accéder à des services commerciaux aux frais d'un autre utilisateur.

* Il existe, sur Internet, des milliers de groupes de discussion spécialisés; la plupart d'entre eux sont ouverts à tout utilisateur. Les articles peuvent contenir des données personnelles concernant des tiers; ces informations personnelles sont enregistrées simultanément sur des milliers de systèmes informatiques, sans que la personne concernée ait aucun droit de regard.

Les participants à Internet ont tous intérêt à l'intégrité et à la confidentialité des informations transmises. Les utilisateurs sont soucieux de la fiabilité des services et s'attendent à voir leur vie privée protégée. Dans certains cas, ils peuvent souhaiter utiliser des services sans être identifiés. Les utilisateurs ne réalisent généralement pas, lorsqu'ils " surfent" sur le Net, qu'ils pénètrent sur un marché mondial, ni que chacun de leur mouvement peut être surveillé.
D'autre part, beaucoup de fournisseurs sont intéressés par l'identification et l'authentification des utilisateurs: ils ont besoin des données personnelles pour la facturation, mais ils pourraient aussi utiliser ces données à d'autres fins. Plus Internet est utilisé à des fins commerciales, plus il est intéressant pour les prestataires de services et pour d'autres organismes d'obtenir le plus possible d'informations générées par les transactions sur le comportement des clients sur le Net, ce qui accroît le risque concernant le secret de la vie privée du client. Des sociétés commencent à offrir de plus en plus souvent un accès gratuit au Net, en vue de s'assurer que les clients vont lire leur publicité, qui devient une méthode de financement majeure pour Internet dans son ensemble. Ces entreprises veulent donc suivre dans quelle mesure, par qui et

avec quelle fréquence leurs publicités sont lues. Concernant certains des risques mentionnés, les fonctions des organismes qui gèrent le Net au plan international, régional et national, sont importantes, en particulier lorsqu'il s'agit de mettre au point les protocoles et les normes destinés à Internet, de fixer les règles d'identification des serveurs connectés et, enfin, pour l'identification des utilisateurs.

II. Réglementations et directives existantes

Si plusieurs gouvernements nationaux et organisations internationales (par exemple l'Union Européenne) ont lancé des programmes pour faciliter et intensifier le développement des réseaux et services informatiques, il n'y a eu que très peu d'efforts pour mettre sur pied des réglementations suffisantes de protection des données et de respect de la vie privée dans ce domaine. Certains services publics nationaux responsables de la protection des données ont déjà publié des directives sur la sécurité technique des réseaux informatiques reliés à Internet et sur les risques encourus par les utilisateurs individuels des services Internet, concernant le secret de leur vie privée. Des directives de ce genre ont été définies, par exemple en France, au Royaume-Uni (voir le "11th Annual Report of the Data Protection Registrar", annexe 6) et en Allemagne. Les principaux sujets abordés peuvent se résumer de la façon suivante :

* La fourniture d'informations sur Internet est soumise aux lois et règlements nationaux de protection des données. A cet égard, Internet n'est pas aussi en dehors des lois qu'on le dit souvent. Pour n'en citer qu'un exemple, il est illicite pour un fournisseur allemand d'un serveur WorlWideWeb d'enregistrer les adresses complètes des ordinateurs qui ont accédé à des pages Web déterminées ou d'enregistrer les fichiers qu'ils ont téléchargés, sans le faire savoir à la personne qui a lancé la procédure (comme il est de pratique courante sur le Net). Les réglementations nationales peuvent comprendre l'obligation pour les fournisseurs d'informations de s'enregistrer auprès d'une autorité nationale de protection des données. La législation nationale contient aussi des dispositions particulières concernant le droit criminel, privé et administratif international (conflit de législations), qui pourraient fournir des solutions dans certains cas.

* Avant de connecter un réseau informatique local – par exemple celui d'un organisme officiel – à Internet, il faut évaluer les risques pour la sécurité du réseau local et des données qui y sont stockées, conformément à la législation nationale. Cela peut obliger à établir un plan de sécurité et à évaluer s'il est nécessaire de connecter l'ensemble du réseau ou uniquement certaines parties de celui-ci à Internet. En fonction de l'objectif, il peut même suffire de ne connecter au Net qu'un système isolé. Des mesures techniques doivent être prises pour s'assurer que seules les données pouvant être publiées seront accessibles sur Internet, par exemple en établissant un système "pare-feu" séparant le réseau local du Net. Il faut cependant noter que même lorsque ce type de mesure technique est prise, la connexion d'un réseau informatique à Internet entraîne des risques supplémentaires pour sa sécurité.

* Si des données personnelles concernant les utilisateurs d'un services sont collectées, il doit être clairement indiqué à ces utilisateurs qui va utiliser les données et à quelles fins elles vont être utilisées ou divulguées. Cela signifie

que les utilisateurs doivent être prévenus à l'écran avant la divulgation des données et qu'il doit leur être possible d'empêcher cette divulgation. L'utilisateur doit pouvoir faire un tirage papier de cet avis et de toutes les autres conditions fixées par le fournisseur.

* Lorsque l'accès à des données personnelles est offert sur un système informatique – par exemple en publiant des détails biographiques sur les membres du personnel dans un annuaire– le fournisseur d'informations doit s'assurer que toutes les personnes concernées comprennent que le monde entier a accès à ces données. La méthode la plus sûre consiste à ne publier les données qu'avec le consentement informé des intéressés.

Il existe aussi un certain nombre de réglementations légales et de conventions internationales qui s'appliquent, entre autres, à Internet.

- Recommandation avec directives sur la protection de la vie privée et des flux transfrontières de données personnelles adoptée par le Conseil de l'Organisation de Coopération et Développement Economique (OCDE) le 23 septembre 1980

- Convention du Conseil de l'Europe N 108 pour la protection des individus concernant le traitement automatique des données personnelles adoptée le 28 janvier 1981
- Directives pour la régulation des fichiers de données personnelles informatiséesadoptées par l'Assemblé générale des Nations Unies le 14 décembre 1990

- Conseil de l'Europe 90/387/EEC du 28 juin 1990 sur l'établissement du marché intérieur des services de télécommunications par la mise en œuvre d'Open Network Provision (ONP) et des directives ONP qui s'ensuivent (définissant la protection des données comme une "exigence essentielle")

- Directive 95/46/EC du Parlement Européen et du Conseil du 24 octobre 1995 sur la protection des personnes concernant le traitement des données personnelles et sur le libre mouvement de ces données (Directive sur la protection des données de l'Union Européenne)

- Accords du GATS (stipulant dans l'article XIV, que les Etats membres ne sont pas empêchés par cet accord mondial d'adopter ou de mettre en vigueur des réglementations concernant la protection de la vie privée des personnes en ce qui concerne le traitement et la diffusion des données personnelles et la protection de la confidentialité d'enregistrements et de comptes individuels.

La Directive de l'Union Européenne, en tant que premier instrument juridique supranational, contient une définition nouvelle importante de "contrôleur", qui est intéressante dans le contexte Internet. L'article 2, alinéa c), définit le "contrôleur" comme la personne, le pouvoir public, l'organisme ou toute autre entité naturelle ou juridique qui, à elle seule ou conjointement à d'autres, détermine les objectifs et les moyens de traitement des données personnelles. Si l'on applique cette définition à l'utilisation d'Internet aux fins de messagerie électronique, l'expéditeur d'un message électronique doit être considéré comme le contrôleur de ce message lorsqu'il envoie

un fichier de données personnelles, car c'est lui qui détermine les objectifs et les moyens de traiter et de transmettre ces données personnelles. D'autre part, le prestataire du service de boîte au lettres détermine les objectifs et les moyens de traitement des données personnelles liés au fonctionnement du service de boîte aux lettres et il assume donc, en tant que "contrôleur", au moins une responsabilité conjointe pour le respect des règles de protection des données applicables.
Plus récemment, la Commission Européenne a publié deux documents qui pourraient aboutir à une législation de l'Union Européenne et qui auraient, dans ce cas, des conséquences considérables sur la protection des données sur Internet:

> Communication au Parlement européen, au Conseil, au Comité économique et social et au Comité des régions sur le contenu illicite et nocif d'Internet (COM(96)487)

et

> Livret vert sur la protection des mineurs et sur la dignité humaine dans les services audiovisuels et informationnels (COM(96)483).

Bien que non légalement contraignants et adoptés au niveau national plutôt qu'au niveau international, les

> –Principes pour la fourniture et l'utilisation d'informations personnelles
> "Privacy and the National Information Infrastructure"
> adoptés par le Privacy Working Group
> de l'Information Policy Committee
> dans le cadre de l'United States Information Infrastructure Task Force (IITF) le 6 juin 1995

doivent être mentionnés dans ce contexte, car ils influeront à coup sûr sur les flux de données internationaux. Ils ont fait l'objet de discussions intenses et fructueuses avec le Groupe de travail international sur la protection des données dans les télécommunications, lors de la réunion conjointe à Washington, D.C., le 28 avril 1995.

En pratique, quelques règles importantes et efficaces sont imposées par l'autorégulation de la communauté Internet elle-même (par exemple "Netiquette"). Ces méthodes ne doivent pas être sous-estimées quant au rôle qu'elles jouent et qu'elles sont susceptibles de jouer à l'avenir dans la protection de la vie privée des utilisateurs individuels. Pour le moins, elles contribuent à la nécessaire sensibilisation des utilisateurs sur la non-existence de la confidentialité en tant que norme fondamentale sur Internet ("N'envoyez et ne conservez jamais rien dans votre boîte aux lettres que vous ne voudriez pas voir publié dans le journal du soir.") La Directive sur la protection des données de l'Union Européenne demande, à son tour, des codes de conduite (article 27) qui devraient être encouragés par les Etats membres et par la Commission.

III. Lignes directrices

Il ne fait aucun doute que la protection juridique et technique de la vie privée des utilisateurs d'Internet est actuellement insuffisante.

D'une part le droit de toute personne à utiliser l'autoroute de l'information sans être observée ni identifiée doit être garanti. D'autre part il doit y avoir des limites (garde-fou) concernant l'utilisation des données personnelles (par exemple de tiers) sur l'autoroute.

Une solution à ce dilemme fondamental devra être trouvée au niveau suivant:

1. Les prestataires de services devraient informer de façon non équivoque chaque utilisateur potentiel du Net des risques concernant le secret de la vie privée. Ce sera alors à l'utilisateur de peser ces risques en fonction des avantages escomptés.

2. Etant donné que "les éléments de l'infrastructure du réseau ainsi que les participants ont chacun un emplacement physique, les Etats ont la possibilité d'imposer et de faire respecter aux réseaux et à leurs participants un certain degré de responsabilité" (Joel Reidenberg). Dans bien des cas, la décision de se brancher sur Internet et la façon de l'utiliser sont soumises à des conditions juridiques dans le cadre de la législation nationale sur la protection des données.

Les données personnelles ne peuvent être collectées que de façon transparente. Les données concernant les patients et les autres données sensibles ne doivent être communiquées par l'intermédiaire d'Internet ou être enregistrées sur des ordinateurs connectés à Internet que si elles sont cryptées.

Il y a aussi une forte opposition à l'utilisation d'Internet pour la publication des avis de recherche par la police (le FBI américain publie depuis un certain temps sur Internet une liste de suspects recherchés et d'autres forces de police nationales suivent cet exemple). Les déficiences décrites dans la procédure d'identification et la facilité de manipulation des images dans un espace cybernétique semblent interdire l'utilisation du Net à cette fin.

3. Plusieurs gouvernements nationaux demandent des accords internationaux sur l'infrastructure informationnelle mondiale. Les initiatives visant à promouvoir une coopération internationale plus étroite et même une convention internationale régissant la protection des données dans le contexte des réseaux et services transfrontières doivent être soutenues.

4. Il est nécessaire de créer un mécanisme de surveillance international qui pourrait s'appuyer sur les structures existantes telles que l'Internet Society et d'autres organismes. La responsabilité de la protection de la vie privée devra être institutionnalisée dans une certaine mesure.

5. La législation nationale et internationale doit stipuler de façon non équivoque que le processus de communication (par exemple par courrier électronique) est également protégée par le secret des télécommunications et de la correspondance.

6. En outre, il est nécessaire d'élaborer des moyens techniques pour améliorer le secret de la vie privée de l'utilisateur sur le Net. Il est indispensable d'élaborer des principes de conception pour la technologie de l'information et des communications et pour le matériel et le logiciel multimédias permettant à l'utilisateur individuel de contrôler l'utilisation de ses données personnelles et d'en obtenir communication en retour. D'une manière générale, les utilisateurs doivent avoir la possibilité d'accéder à

Internet sans devoir révéler leur identité, lorsque les données personnelles ne sont pas nécessaires à la prestation d'un service déterminé. Les principes de mesures de ce type ont déjà été élaborés et publiés. En voici des exemples: le principe du "Protecteur d'identité" qui se trouve dans "Technologies pour améliorer le secret de la vie privée: la voie vers l'anonymat" publié par le Dutch Registratiekamer et The Information and Privacy Commissioner of Ontario/Canada, présenté à la 17e Conférence internationale sur la protection des données, à Copenhague (1995) et le "Concept d'agent-utilisateur" mentionné à la réunion conjointe du Groupe de travail et du Privacy Working Group de l'IITF (avril 1995), à Washington.

7. Des moyens techniques doivent aussi être mis en œuvre en vue de protéger la confidentialité. En particulier l'utilisation de méthodes sûres de cryptage doit devenir et rester une option légitime pour tout utilisateur d'Internet.

L'utilisation de méthodes sûres de cryptage doit devenir et rester une option légitime pour tout utilisateur d'Internet.

Le Groupe de travail soutient les nouvelles évolutions du protocole Internet (par exemple IPv6) qui offrent des moyens d'améliorer la confidentialité par cryptage, classification de messages et de meilleures méthodes d'authentification. Les éditeurs de logiciels doivent mettre en œuvre la nouvelle norme de sécurité de l'Internet Protocol dans leurs produits et les prestataires de services doivent soutenir l'utilisation de ces produits aussi rapidement que possible.

8. Le Groupe de travail soutiendrait une étude de faisabilité concernant la mise au point d'une nouvelle méthode de certification délivrant des "labels de qualité" aux fournisseurs et aux produits pour leur aptitude à la protection du secret de la vie privée. Cela pourrait aboutir à améliorer la transparence pour les utilisateurs des autoroutes de l'information.

9. L'anonymat est un élément complémentaire essentiel à la protection de la vie privée sur Internet. Les limitations du principe de l'anonymat doivent être strictement limitées à ce qui est nécessaire dans une société démocratique, sans remettre en question le principe en lui-même.

10. Enfin, un élément décisif consistera à étudier comment une autorégulation reposant sur une "Netiquette" étendue et une technologie favorable au secret de la vie privée sont susceptibles d'améliorer la mise en œuvre des réglementations nationales et internationales sur la protection de la vie privée. Il ne suffira pas de s'en remettre à un seul de ces modes d'action: ils devront être combinés de façon efficace pour parvenir à une infrastructure d'information mondiale respectant les droits de l'Homme au secret de la vie privée et à des communications non surveillées.

Le Groupe de travail international sur la protection des données dans les télécommunications surveillera de près les progrès dans ce domaine, tiendra compte des remarques émanant de la communauté Internet et élaborera de nouvelles propositions plus détaillées.

4. Recommandation du Conseil de l'Europe relative à la protection des données médicales

RECOMMANDATION N? R (97) 5

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES

RELATIVE À LA PROTECTION DES DONNÉES MÉDICALES

(adoptée par le Comité des Ministres le 13 février 1997, lors de la 584e réunion des Délégués des Ministres)

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

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

Rappelant les principes généraux relatifs à la protection des données de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Série des traités européens, n? 108), notamment son article 6 qui énonce que les données à caractère personnel relatives à la santé ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées;

Conscient du fait que le traitement automatisé des données médicales par des systèmes d'information est de plus en plus répandu non seulement pour les soins médicaux, la recherche médicale, la gestion hospitalière et la santé publique, mais également en dehors du secteur des soins de santé;

Convaincu de l'importance que la qualité, l'intégrité et la disponibilité des données médicales revêtent pour la santé de la personne concernée et de ses proches;

Conscient du fait que les progrès des sciences médicales dépendent dans une large mesure de la disponibilité des données médicales des individus;

Persuadé qu'il est souhaitable de réglementer la collecte et le traitement des données médicales, de garantir le caractère confidentiel et la sécurité des données à caractère personnel relatives à la santé, et de veiller à ce qu'il en soit fait un usage respectant les droits et les libertés fondamentales de l'individu, notamment le droit à la vie privée;

Conscient du fait que les progrès accomplis dans les sciences médicales et les développements intervenus dans la technologie de l'information depuis 1981 nécessitent la révision de plusieurs dispositions de la Recommandation n? R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées,

Recommande aux gouvernements des Etats membres :

- de prendre des mesures pour que les principes contenus dans l'annexe à la présente recommandation se reflètent dans leur droit et leur pratique;

- d'assurer une large diffusion des principes contenus dans l'annexe à la présente recommandation parmi les personnes qui collectent et traitent des données médicales à titre professionnel;

Décide que la présente recommandation remplace la Recommandation n? R (81) 1 relative à la réglementation applicable aux banques de données médicales automatisées.

Annexe à la Recommandation N? R (97) 5

1. Définitions

Aux fins de la présente recommandation:

- l'expression «données à caractère personnel» signifie toute information concernant une personne physique identifiée ou identifiable. Une personne physique n'est pas considérée comme identifiable si cette identification nécessite des délais et des activités déraisonnables. Lorsqu'une personne physique n'est pas identifiable, les données sont dites anonymes;

- l'expression «données médicales» se réfère à toutes les données à caractère personnel relatives à la santé d'une personne. Elle se réfère également aux données ayant un lien manifeste et étroit avec la santé ainsi qu'aux données génétiques;

- l'expression «données génétiques» se réfère à toutes les données, quel qu'en soit le type, qui concernent les caractères héréditaires d'un individu ou qui sont en rapport avec de tels caractères formant le patrimoine d'un groupe d'individus apparentés.

Elle se réfère également à toute donnée portant sur l'échange de toute information génétique (gènes) concernant un individu ou une lignée génétique, en rapport avec les aspects, quels qu'ils soient, de la santé ou d'une maladie, qu'elle constitue ou non un caractère identifiable.

La lignée génétique est constituée par des similitudes génétiques résultant d'une procréation et partagées par deux ou plusieurs individus.

2. Champ d'application

2.1. La présente recommandation est applicable à la collecte et au traitement automatisé de données médicales, à moins que le droit interne, dans un contexte spécifique hors du domaine des soins de santé, ne prévoie d'autres garanties appropriées.

2.2. Un Etat membre peut étendre les principes énoncés dans la présente recommandation aux données médicales ne faisant pas l'objet d'un traitement automatisé.

3. Respect de la vie privée

3.1. Le respect des droits et des libertés fondamentales et notamment du droit à la vie privée, doit être garanti lors de la collecte et du traitement des données médicales.

3.2. Les données médicales ne peuvent être collectées et traitées que conformément aux garanties appropriées qui doivent être prévues par le droit interne.

En principe, la collecte et le traitement de données médicales ne devraient être effectués que par des professionnels des soins de santé ou par des personnes ou organismes agissant pour le compte de professionnels des soins de santé. Les personnes ou organismes agissant pour le compte de professionnels des soins de santé qui collectent et traitent des données médicales devraient être soumis aux règles de confidentialité propres aux professionnels des soins de santé ou à des règles de confidentialité comparables.

Les maîtres des fichiers qui ne sont pas des professionnels des soins de santé ne devraient collecter et traiter des données médicales que dans le respect soit de règles de confidentialité comparables à celles incombant à un professionnel des soins de santé, soit des garanties d'efficacité égales prévues par le droit interne.

4. Collecte et traitement de données médicales

4.1. La collecte et le traitement des données médicales doivent être effectués de manière loyale et licite, et uniquement pour des finalités déterminées.

4.2. Les données médicales doivent en principe être collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources que conformément aux chapitres 4, 6 et 7, et à condition que cela soit nécessaire pour réaliser la finalité du traitement ou que la personne concernée ne soit pas en mesure de fournir les données.

4.3. Les données médicales peuvent être collectées et traitées:

a. si la loi le prévoit:

i. aux fins de la santé publique; ou
ii. sous réserve du principe 4.8, aux fins de la prévention d'un danger concret ou pour la répression d'une infraction pénale déterminée; ou
iii. aux fins d'un autre intérêt public important; ou

b. dans la mesure où la loi l'autorise:

i. à des fins médicales préventives, ou à des fins diagnostiques ou thérapeutiques à l'égard de la personne concernée ou d'un parent de la lignée génétique; ou
ii. aux fins de sauvegarde des intérêts vitaux de la personne concernée ou d'une tierce personne; ou
iii. aux fins du respect d'une obligation contractuelle spécifique; ou
iv. aux fins de la constatation, de l'exercice ou de la défense d'un droit en justice; ou

c. si la personne concernée ou son représentant légal ou une autorité ou toute personne ou instance désignée par la loi y a consenti, pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas.

4.4. Lorsque les données médicales ont été collectées à des fins médicales préventives, ou à des fins diagnostiques ou thérapeutiques à l'égard de la personne concernée ou d'un parent de la lignée génétique, elles peuvent également être traitées à des fins de gestion d'un service de santé agissant dans l'intérêt du patient, dans le cas où la gestion est fournie par le professionnel des soins de santé qui a collecté les données, ou lorsque les données sont communiquées conformément aux dispositions énoncées aux principes 7.2 et 7.3.

Enfant à naître

4.5. Les données médicales relatives à un enfant à naître devraient être considérées comme des données à caractère personnel et jouir d'une protection comparable à celle des données médicales d'un mineur.

4.6. A moins que le droit interne n'en dispose autrement, le détenteur des responsabilités parentales peut agir en qualité de personne habilitée juridiquement à agir pour un enfant à naître en tant que personne concernée.

Données génétiques

4.7. Les données génétiques collectées et traitées à des fins de prévention, de diagnostic, ou à des fins thérapeutiques à l'égard de la personne concernée ou pour la recherche scientifique, ne devraient être utilisées qu'à ces seules fins ou pour permettre à la personne concernée de prendre une décision libre et éclairée à leur sujet.

4.8. Le traitement des données génétiques pour les besoins d'une procédure judiciaire ou d'une enquête pénale devrait faire l'objet d'une loi spécifique offrant des garanties appropriées.

Ces données devraient servir exclusivement à la vérification de l'existence d'un lien génétique dans le cadre de l'administration de la preuve, à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. En aucun cas elles ne devraient être utilisées pour déterminer d'autres caractéristiques qui peuvent être liées génétiquement.

4.9. A des fins autres que celles prévues aux principes 4.7 et 4.8, la collecte et le traitement des données génétiques devraient en principe être permis uniquement pour des raisons de santé et notamment pour éviter tout préjudice sérieux à la santé de la personne concernée ou de tiers.

Cependant, la collecte et le traitement des données génétiques en vue de dépister des maladies peuvent être permis en cas d'intérêt supérieur et à condition qu'il existe des garanties appropriées définies par la loi.

5. Information de la personne concernée

5.1. La personne concernée doit être informée des éléments suivants:

a. l'existence d'un fichier contenant ses données médicales et la catégorie de données collectées ou à collecter;

b. la ou les finalités pour lesquelles ces données sont ou seront traitées;

c. le cas échéant, les personnes ou les organismes auprès desquels elles sont ou seront collectées;

d. les personnes ou les organismes auxquels - et les objectifs pour lesquels - elles peuvent être communiquées;

e. la possibilité, le cas échéant, pour la personne concernée de refuser son consentement, de le retirer, et les conséquences d'un tel retrait;

f. l'identité du maître de fichier et, le cas échéant, de son représentant, ainsi que les conditions d'exercice du droit d'accès et de rectification.

5.2. La personne concernée devrait être informée au plus tard au moment de la collecte. Toutefois, lorsque les données médicales ne sont pas collectées auprès de la personne concernée, celle-ci devrait être informée de la collecte le plus rapidement possible ainsi que, de manière appropriée, des éléments mentionnés au principe 5.1, sauf si cela est manifestement déraisonnable ou infaisable, ou si la personne concernée a déjà reçu l'information.

5.3. L'information de la personne concernée doit être appropriée et adaptée aux circonstances. Chaque personne concernée devrait, de préférence, être informée individuellement.

5.4. Avant qu'une analyse génétique soit effectuée, la personne concernée devrait être informée des objectifs de l'analyse et de l'éventualité de découvertes inattendues.

Incapables légaux

5.5. Si la personne concernée est une personne légalement incapable et n'est pas en mesure de se déterminer librement, et si le droit interne ne lui permet pas d'agir en son propre nom, l'information doit être donnée à la personne pouvant agir légalement dans l'intérêt de la personne concernée.

Si elle est en mesure de comprendre, la personne légalement incapable devrait être informée avant que les données qui la concernent soient collectées ou traitées.

Dérogations

5.6. Des dérogations aux principes 5.1, 5.2 et 5.3 peuvent être faites dans les cas suivants:

a. l'information de la personne concernée peut être limitée, si la dérogation est prévue par la loi et qu'elle constitue une mesure nécessaire dans une société démocratique:

i. à la prévention d'un danger concret ou à la répression d'une infraction pénale;
ii. pour des raisons de santé publique;
iii. à la protection de la personne concernée et des droits et libertés d'autrui;

b. en cas d'urgence médicale, les données considérées comme étant nécessaires au traitement médical peuvent être collectées avant l'information.

6. Consentement

6.1. Lorsque la personne concernée est appelée à donner son consentement, celui-ci devrait être libre, exprès et éclairé.

6.2. Les résultats de toute analyse génétique devraient être formulés dans les limites des objectifs de la consultation médicale, du diagnostic ou du traitement pour lesquels le consentement a été obtenu.

6.3. Lorsque l'on envisage de traiter des données médicales concernant une personne légalement incapable qui n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne permet pas à la personne concernée d'agir en son propre nom, le consentement de la personne pouvant agir légalement au nom de la personne concernée, ou d'une autorité, ou de toute personne ou instance désignée par la loi, est requis.

Si, conformément au principe 5.5 ci-dessus, la personne légalement incapable a été informée de l'intention de collecter ou de traiter ses données médicales, son souhait devrait être pris en considération, à moins que le droit interne ne s'y oppose.

7. Communication

7.1. Les données médicales ne doivent pas être communiquées, sauf dans les conditions énumérées dans le présent chapitre et dans le chapitre 12.

7.2. En particulier, à moins que le droit interne ne prévoie d'autres garanties appropriées, la communication des données médicales ne peut intervenir que si le destinataire est soumis aux règles de confidentialité propres aux professionnels des soins de santé ou à des règles de confidentialité comparables, et seulement s'il respecte les dispositions de la présente recommandation.

7.3. Les données médicales peuvent être communiquées si elles sont pertinentes et:

a. si la communication est prévue par la loi et constitue une mesure nécessaire dans une société démocratique aux fins:

i. de la santé publique; ou
ii. de la prévention d'un danger concret ou pour la répression d'une infraction pénale déterminée; ou
iii. d'un autre intérêt public important; ou
iv. de la protection des droits et libertés d'autrui; ou

b. si la loi autorise la communication aux fins:

i. de la protection de la personne concernée ou d'un parent de la lignée génétique; ou
ii. de la sauvegarde des intérêts vitaux de la personne concernée ou d'une tierce personne; ou
iii. du respect d'obligations contractuelles spécifiques; ou
iv. de la constatation, de l'exercice ou de la défense d'un droit en justice; ou

c. si la personne concernée ou son représentant légal, ou une autorité, ou toute personne ou instance désignée par la loi, y a consenti pour une ou plusieurs finalités et pour autant que le droit interne ne s'y oppose pas;

d. à moins que la personne concernée ou son représentant légal, ou une autorité, ou toute personne ou instance désignée par la loi, ne s'y soit expressément opposée lorsque la communication n'est pas obligatoire, si les données ont été collectées dans un contexte préventif, diagnostique ou thérapeutique librement choisi et si la finalité de la communication n'est pas incompatible avec la finalité du traitement pour laquelle ces données ont été collectées, notamment aux fins d'accomplissement de soins au patient ou de gestion d'un service de santé agissant dans l'intérêt du patient.

8. Droits de la personne concernée

Droits d'accès et de rectification

8.1. Toute personne doit pouvoir accéder aux données médicales la concernant, soit directement, soit par l'intermédiaire d'un professionnel des soins de santé ou, si le droit interne le permet, par l'intermédiaire d'une personne désignée par elle. Les informations doivent être accessibles sous une forme compréhensible.

8.2. L'accès aux données médicales peut être refusé, limité ou différé uniquement si la loi le prévoit et:

a. si cela constitue une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'Etat, à la sûreté publique ou à la répression des infractions pénales; ou

b. si la connaissance de ces informations est susceptible de causer une atteinte grave à la santé de la personne concernée; ou

c. si l'information sur la personne concernée révèle également des informations sur des tiers ou, en ce qui concerne les données génétiques, si ces informations sont susceptibles de porter une atteinte grave à des parents consanguins ou utérins, ou à une personne ayant un lien direct avec cette lignée génétique; ou

d. si les données sont utilisées à des fins de statistiques ou de recherches scientifiques lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées, notamment du fait que les données ne sont pas utilisées pour des décisions ou des mesures relatives à une personne déterminée.

8.3. La personne concernée peut demander la rectification de données erronées la concernant et, en cas de refus, doit pouvoir faire recours.

Découvertes inattendues

8.4. La personne soumise à une analyse génétique devrait être informée des découvertes inattendues si les conditions suivantes ont été remplies:

a. le droit interne n'interdit pas une telle information;

b. la personne a fait la demande explicite de cette information;

c. l'information n'est pas susceptible de porter une atteinte grave:

i. à la santé de la personne; ou
ii. à un parent consanguin ou utérin de la personne, à un membre de sa famille sociale, ou à une personne ayant un lien direct avec la lignée génétique de la personne, à moins que le droit interne ne prévoie d'autres garanties appropriées.

Sous réserve de l'alinéa a, la personne devrait également être informée si ces découvertes revêtent pour elle une importance thérapeutique ou préventive directe.

9. *Sécurité*

9.1. Des mesures techniques et d'organisation appropriées doivent être prises pour la protection des données à caractère personnel traitées conformément à la présente recommandation contre la destruction — accidentelle ou illicite — et la perte accidentelle, ainsi que contre l'accès, la modification, la communication ou toute autre forme de traitement non autorisés.

Ces mesures doivent assurer un niveau de sécurité approprié compte tenu, d'une part, de l'état de la technique et, d'autre part, de la nature sensible des données médicales et de l'évaluation des risques potentiels.

Ces mesures doivent faire l'objet d'un examen périodique.

9.2. Afin notamment d'assurer la confidentialité, l'intégrité et l'exactitude des données traitées, ainsi que la protection des patients, des mesures appropriées devraient être prises visant:

a. à empêcher toute personne non autorisée d'accéder aux installations utilisées pour le traitement de données à caractère personnel (contrôle à l'entrée des installations);

b. à empêcher que des supports de données puissent être lus, copiés, modifiés ou déplacés par une personne non autorisée (contrôle des supports de données);

c. à empêcher l'introduction non autorisée de données dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données à caractère personnel mémorisées (contrôle de mémoire);

d. à empêcher que des systèmes de traitement automatisé de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données (contrôle de l'utilisation);

e. en vue, d'une part, de l'accès sélectif aux données et, d'autre part, de la sécurité des données médicales, à assurer que leur traitement soit en règle générale conçu de façon à permettre la séparation:

— des identifiants et des données relatives à l'identité des personnes,
— des données administratives,
— des données médicales,
— des données sociales,
— des données génétiques (contrôle d'accès);

f. à garantir qu'il puisse être vérifié et constaté à quelles personnes ou à quels organismes des données à caractère personnel peuvent être communiquées par des installations de transmission de données (contrôle de la communication);

g. à garantir qu'il puisse être vérifié et constaté *a posteriori* qui a eu accès au système et quelles données à caractère personnel ont été introduites dans le système d'information, à quel moment et par quelle personne (contrôle de l'introduction);

h. à empêcher que, lors de la communication de données à caractère personnel ainsi que lors du transport de supports de données, les données puissent être lues, copiées, modifiées ou effacées de façon non autorisée (contrôle du transport);

i. à sauvegarder les données par la constitution de copies de sécurité (contrôle de disponibilité).

9.3. Les maîtres des fichiers médicaux devraient, conformément au droit interne, établir un règlement interne approprié dans le respect des principes pertinents de la présente recommandation.

9.4. Si nécessaire, les maîtres des fichiers qui traitent des données médicales devraient désigner une personne indépendante responsable de la sécurité des

systèmes d'information et de la protection des données, et compétente pour donner des conseils en la matière.

10. Conservation

10.1. En règle générale, les données médicales ne doivent être conservées que pendant la durée nécessaire pour atteindre le but pour lequel elles ont été collectées et traitées.

10.2. Lorsque la conservation de données médicales qui ne sont plus utilisées pour le but d'origine se révèle nécessaire dans l'intérêt légitime de la santé publique, de la science médicale, du responsable du traitement médical ou du maître du fichier aux fins de lui permettre d'exercer ou de défendre ses droits en justice, ou à des fins historiques ou statistiques, des dispositions techniques doivent être prises pour assurer la conservation et la sécurité correctes des données en tenant compte de la vie privée du patient.

10.3. Sur demande de la personne concernée, ses données médicales devraient être effacées, à moins qu'elles ne soient rendues anonymes ou que des intérêts supérieurs et légitimes, et en particulier ceux énoncés au principe 10.2, ou des obligations d'archivage ne s'y opposent.

11. Flux transfrontières

11.1. Les principes de la présente recommandation sont applicables aux flux transfrontières de données médicales.

11.2. Les flux transfrontières de données médicales vers un Etat ayant ratifié la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et disposant d'une législation qui assure une protection des données médicales pour le moins équivalente ne devraient pas être soumis à des conditions particulières de protection de la vie privée.

11.3. Lorsque la protection des données médicales peut être considérée comme étant en harmonie avec le principe de la protection équivalente énoncé dans ladite convention, il ne devrait pas y avoir de limitation aux flux transfrontières de données médicales vers un Etat n'ayant pas ratifié la convention, mais assurant une protection conforme aux principes de ladite convention et de la présente recommandation.

11.4. A moins que le droit interne n'en dispose autrement, les flux transfrontières de données médicales vers un Etat n'assurant pas une protection conforme à ladite convention et à la présente recommandation ne devraient en règle générale pas intervenir, à moins:

a. que des mesures nécessaires, y compris de nature contractuelle, au respect des principes de la convention et de la présente recommandation n'aient été prises et que la personne concernée n'ait la possibilité de s'opposer au transfert; ou

b. que la personne concernée n'ait donné son consentement.

11.5. Sauf en cas d'urgence ou de transfert accepté par la personne concernée après information, lorsque des données médicales sont transférées d'un pays à un autre, des mesures appropriées devraient être prises pour assurer leur protection, en particulier:

a. le responsable du transfert devrait indiquer au destinataire les finalités déterminées et légitimes pour lesquelles les données ont été initialement collectées, ainsi que les personnes ou organismes auxquels elles peuvent être communiquées;

b. sauf si le droit interne en dispose autrement, le destinataire devrait s'engager auprès du responsable du transfert à respecter les finalités déterminées et légitimes reconnues, et à ne pas communiquer ces données à des personnes ou organismes autres que ceux indiqués par le responsable du transfert.

12. Recherche scientifique

12.1. Dans la mesure du possible, les données médicales utilisées à des fins de recherche scientifique devraient être anonymes. Les organisations professionnelles et scientifiques ainsi que les autorités publiques devraient promouvoir le développement de techniques et de procédures assurant l'anonymat.

12.2. Toutefois, si l'anonymisation devait rendre impossible un projet de recherche scientifique et si ce projet devait être effectué dans un but légitime, la recherche pourrait être faite avec des données à caractère personnel, à condition:

a. que la personne concernée ait donné son consentement informé pour la ou les finalités de la recherche; ou

b. que, lorsque la personne concernée est légalement incapable et n'est pas en mesure de se déterminer librement, et lorsque le droit interne ne lui permet pas d'agir en son propre nom, son représentant légal ou une autorité, ou toute personne ou instance désignée par la loi, ait donné son consentement dans le cadre d'un projet de recherche lié à la condition médicale ou à une maladie de la personne concernée; ou

c. que la communication des données aux fins d'un projet de recherche scientifique déterminé pour des raisons d'intérêt public important ait été autorisée par un ou plusieurs organismes désignés par le droit interne, mais seulement:

i. si la personne concernée ne s'est pas expressément opposée à la communication; et

ii. s'il s'avère irréalisable, malgré des efforts raisonnables, de prendre contact avec la personne concernée pour recueillir son consentement; et

iii. si les intérêts du projet de recherche justifient cette autorisation; ou

d. que la recherche scientifique soit prévue par la loi et qu'elle constitue une mesure nécessaire pour des raisons de santé publique.

12.3. Sous réserve de conditions complémentaires prévues par le droit interne, les professionnels des soins de santé habilités à mener leurs propres recherches médicales devraient pouvoir utiliser les données médicales qu'ils détiennent pour autant que la personne concernée ait été informée de cette faculté et ne s'y soit pas opposée.

12.4. A l'égard de toute recherche scientifique fondée sur des données à caractère personnel, les problèmes incidents engendrés par le respect des dispositions de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, y compris ceux de nature éthique et scientifique, devraient également être examinés à la lumière d'autres instruments pertinents.

12.5. Les données à caractère personnel utilisées à des fins de recherche scientifique ne peuvent être publiées sous une forme permettant d'identifier les personnes concernées à moins que ces dernières n'aient donné leur consentement en vue de la publication et que le droit interne autorise cette publication.

5. Dispositions de protection des données dans des lois au sens formel

Voir page 103

6. Recommandations du Préposé fédéral à la protection des données

Voir pages 104 ss