Préposé fédéral à la protection des données

Rapport d'activités 1994/95

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 1994 au 31 mars 1995.

TABLES DE MATIERES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

REPERTOIRE DES ABREVIATIONS

AUPER	Système d'enregistrement automatisé des personnes
AVS	Assurance vieillesse et survivants
BD	Banques des données
CC	Centre de calcul
CJ-PD	Groupe de projets sur la protection des données
CO	Code des obligations
DFJP	Département fédéral de justice et police
DOSIS	(Projet-pilote) Système provisoire de traitement des données en matière de drogue
ISIS	Système provisoire de traitement des données relatives à la protection de l'Etat
LPD	Loi fédérale sur la protection des données
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
MP	Ministère Public
OCDE	Organisation de coopération et de développement économique
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
PF	Police Fédérale
PFPD	Préposé fédéral à la protection des données
RCE	Registre central des étrangers
REGI	Gestion informatisée des personnes et des dossiers
RIPOL	Système de recherches informatisées de police
RNIS	Réseau numérique à intégration de services
TED	Traitement électronique de données

PREFACE

La loi fédérale sur la protection des données (LPD) est entrée en vigueur il y a presque deux ans et le préposé fédéral à la protection des données (PFPD) présente ici son second rapport d'activités. L'exercice écoulé a été marqué par des développements structurels au sein du Secrétariat du PFPD. Nous avons en particulier consacré nos travaux à la procédure de déclaration des fichiers, à l'établissement du registre des fichiers ainsi qu'à son informatisation et sa publication. En outre, le Secrétariat a répondu à une quantité de questions émanant d'organes fédéraux et de particuliers sur des problèmes actuels relevant de la protection des données.

Il s'est à nouveau confirmé que la protection des données ne peut être assurée sur la seule base de principes matériels; elle requiert en fait un dialogue constant tant avec les personnes concernées qu'avec celles traitant les données. Notre action de persuasion revêt à cet égard une importance de plus en plus grande. Lorsqu'un traitement de données personnelles génère une atteinte à la personnalité, elle est en général plutôt due à un manque de sensibilité pour ce genre d'atteinte qu'à un mépris délibéré des principes régissant le traitement des données.

Nous avons en outre constaté que bon nombre d'autorités fédérales et de maîtres de fichiers privés ont reconnu la nécessité de protéger les données personnelles et sont prêts à promouvoir la protection des données. Néanmoins, dans le cadre des débats sur la lutte contre le crime organisé, le droit de l'individu de décider lui-même du sort réservé aux données le concernant est très nettement passé au second plan. D'où la nécessité pour nous, cette année encore, de mettre l'accent sur notre action de persuasion, outre les efforts visant le respect des exigences de la LPD.

Les méthodes de traitement des données personnelles et les possibilités offertes à cet égard évoluent de manière très diverse. En Suisse, de nouveaux systèmes voient sans cesse le jour - c'est d'ailleurs un phénomène mondial -. Ils contiennent toujours plus de données personnelles et limitent d'autant le droit des personnes concernées à l'autodétermination en matière d'information. Mentionnons simplement les nouveaux systèmes de police et de sécurité. Le danger vient également d'autres domaines comme la surveillance téléphonique sur le lieu de travail ou les possibilités d'utilisation illimitées du trafic des paiements sans espèces (cartes à puce ou télébanking). En effet, le trafic électronique des paiements permet, du moins en cas d'utilisation fréquente, l'établissement de banques de données grâce à la consultation des mouvements de paiement, lesquels donnent une vue complète des "habitudes" des détenteurs de cartes et peuvent même générer des profils de la personnalité.

Dans notre société, le traitement des données personnelles prendra indéniablement une place de plus en plus grande du fait du développement des technologies. Le but n'est pas de limiter ou d'empêcher le flot d'informations, mais de lier l'utilisation des données personnelles à une stricte finalité. Tel est l'objectif fondamental de la protection des données : elle n'entend pas interdire le traitement des données, mais le permettre uniquement à la condition qu'il réponde à une fin strictement déterminée.

I. THEMES CHOISIS

1. Affaires de police

1.1. Crime organisé - le nouveau droit d'accès indirect

Le Parlement a adopté, le 7 octobre 1994, la nouvelle loi fédérale sur les Offices centraux de police criminelle de la Confédération. Cette loi est le résultat d'un processus législatif au cours duquel les débats se sont principalement focalisés sur le problème particulier de l'exercice du droit d'accès. En effet, suite aux réserves ques nous avons émises aux restrictions du droit d'accès introduites dans le Message du Conseil fédéral concernant la modification du code pénal en vue de la création d'un office central de lutte contre le crime organisé, le Parlement s'est également saisi de cette problématique et en a longuement débattu. Il a finalement opté pour l'élaboration d'une loi propre à la lutte contre le crime organisé et a adopté une disposition spécifique au droit d'accès dérogeant aux règles de la loi fédérale sur la protection des données. Cette norme instaure un droit d'accès indirect, prévoyant notre intervention en tant qu'autorité chargée de vérifier si les données ont été traitées par les offices centraux conformément au droit. Cette disposition est en outre applicable aux demandes de renseignements concernant le système DOSIS.

L'engagement politique déployé en faveur d'un renforcement de la législation destinée à lutter plus efficacement contre les nouvelles formes de criminalité, en particulier la criminalité économique et le crime organisé, a abouti, le 7 octobre 1994, à l'adoption de la loi fédérale sur les Offices centraux de police criminelle de la Confédération. Entrée en vigueur le 15 mars 1995, cette nouvelle loi est le résultat de l'examen par le Parlement du Message concernant la création d'un Office central de lutte contre le crime organisé adopté par le Conseil fédéral le 12 janvier 1994. Elle vient compléter le "premier train de mesures" contre le crime organisé constitué des normes pénales sur le blanchiment d'argent sale et le défaut de vigilance dans les opérations financières, ainsi que le "second train de mesures" portant principalement sur le droit de communication du financier et sur la notion d'organisation criminelle.

Cette loi sur les Offices centraux de police criminelle de la Confédération vise principalement à régler les tâches des office centraux de l'Office fédéral de la police dans leur lutte contre le crime organisé international. Elle règle le détachement des agents de liaison à l'étranger, la collaboration avec les autorités de poursuite pénale et les services de police des cantons et de l'étranger ainsi que le traitement des données et les échanges nationaux et internationaux d'informations de police criminelle. Elle définit en outre les tâches de l'Office central de lutte contre le crime organisé et de l'Office central de lutte contre le trafic illicite des stupéfiants. Dans le cadre de la section consacrée au traitement des données personnelles, outre des dispositions sur les systèmes de traitement des données, sur la participation des cantons et sur la communication des données, la loi sur les Offices centraux de police criminelle contient un article 14 intitulé: "Information des personnes concernées et communication des renseignements".

Cette disposition particulière est le fruit de très longs débats au sein du Parlement. Dans un premier temps, le Message du Conseil fédéral concernant la création d'un

office central de lutte contre le crime organisé prévoyait une disposition particulière inspirée de la législation allemande: ainsi la personne concernée souhaitant exercer son droit d'accès aurait dû faire valoir un état de faits concret et invoquer un intérêt particulier à l'information. Ne pouvant approuver de telles conditions, nous avons rappelé que l'obligation d'invoquer un intérêt particulier peut à la rigueur être justifiée dans le cadre de la lutte contre le crime organisé, bien qu'elle se heurte à la jurisprudence du Tribunal fédéral. Celle-ci stipule que celui qui prétend avec quelque vraisemblance que des renseignements personnels enregistrés à son sujet sont susceptibles de porter atteinte à sa liberté personnelle doit pouvoir en requérir la consultation sans avoir à justifier encore d'un autre intérêt digne de protection. Mais c'est surtout la condition imposée à la personne concernée de se référer à un état de faits concret qui n'était de notre point de vue pas acceptable. En effet cette condition revient, de manière contraire à la dignité humaine, à contraindre chaque citoyen à s'accuser de certains faits. De plus, dans la pratique cette condition sera dans la majorité des cas impossible à remplir pour le citoyen qui n'a rien à se reprocher mais qui souhaiterait vérifier qu'il ne fait pas l'objet d'une surveillance policière abusive ou infondée. Nous avons enfin rappelé qu'une telle solution entrée en vigueur en Allemagne en décembre 1990 avait, lors de son adoption, fait l'objet d'oppositions, et qu'après quelques années d'expérience, elle reste toujours sous le feu de la critique, notamment du Préposé fédéral allemand à la protection des données.

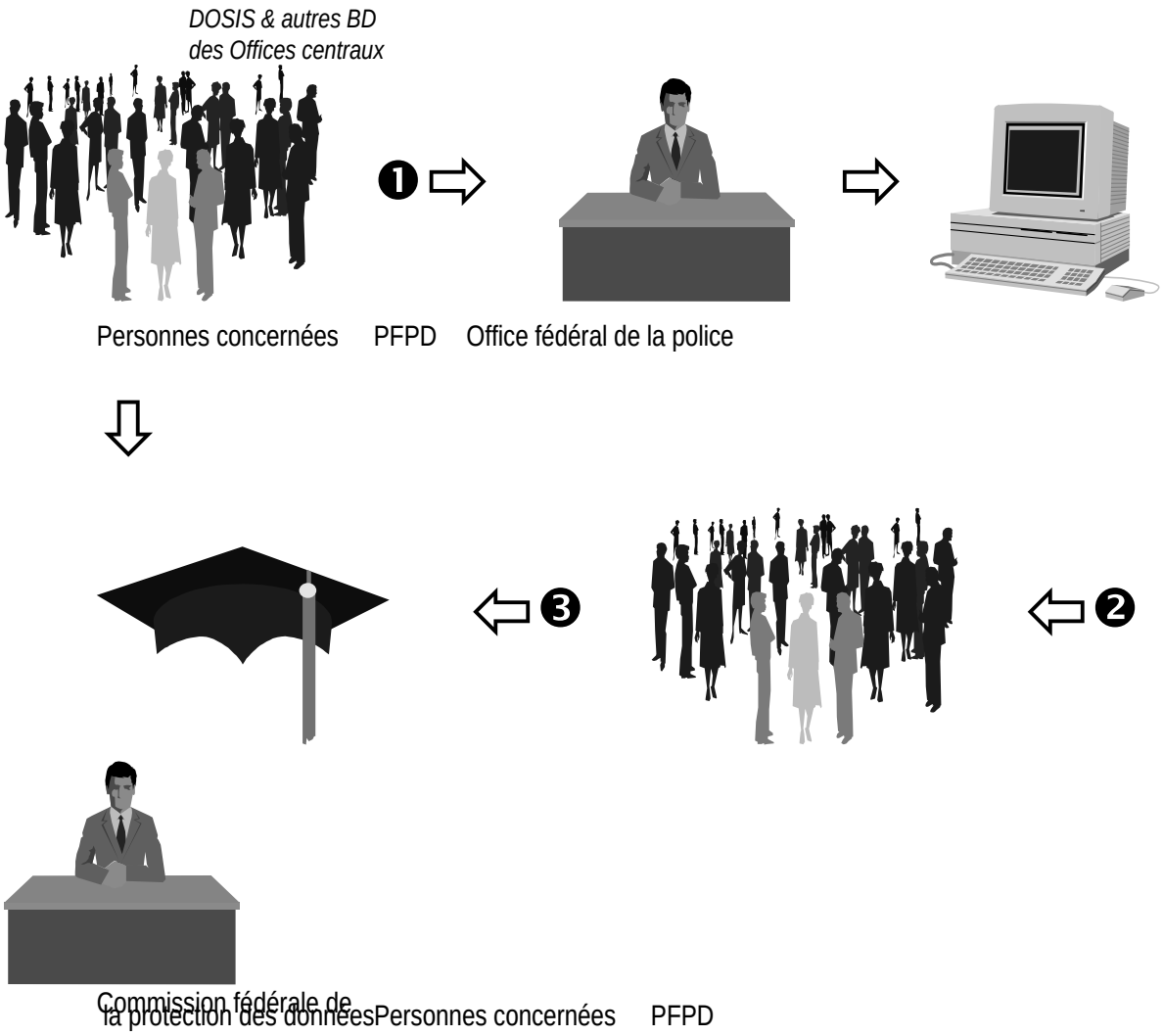
Nos réserves émises dans le cadre de différentes prises de position ont été discutées par les Chambres fédérales lorsque celles-ci ont examiné le projet de loi. Nous avons en outre été invités à donner notre point de vue sur cette problématique en Commission parlementaire. Nous avons ainsi eu l'occasion de présenter aux parlementaires les différents mécanismes mis en place dans les autres législations nationales et de nous exprimer sur leur fonctionnement. Outre le système inspiré du droit allemand proposé par le Conseil fédéral, ont été étudiées les solutions des droits anglais et français. Ce dernier prévoit notamment un droit d'accès indirect exercé par l'intermédiaire de la Commission nationale de l'informatique et des libertés (CNIL) qui notifie au requérant qu'elle a procédé aux vérifications requises. Un décret permet à la CNIL, avec l'accord du Ministre de l'intérieur, de communiquer à la personne concernée certaines informations collectées par les services des renseignements généraux. L'intéressé dispose en outre de différentes voies de droit en cas de refus d'accès. Durant les débats parlementaires, le système britannique a également été régulièrement mentionné. Il prévoit la nomination d'un tribunal spécial (security service Tribunal) chargé de traiter les plaintes relatives aux activités des services de sécurité, ainsi que d'un préposé spécial (security service Commissionner) exerçant un droit de regard et chargé d'assister le tribunal.

Le Parlement a finalement décidé de s'inspirer des systèmes britannique et français en adoptant l'article 14 de la loi sur les Offices centraux de police criminelle de la Confédération. Cette disposition spéciale, dérogeant aux règles de la loi fédérale sur le protection des données, met en place un mécanisme de *droit d'accès indirect* qui peut être exercé par notre intermédiaire. Il nous paraît nécessaire de souligner que cette procédure n'est applicable qu'aux cas relevant de la loi sur les Offices centraux de police criminelle de la Confédération, dont l'accès au système DOSIS. L'ordonnance réglementant ce système provisoire de traitement des données en matière de lutte contre le trafic illicite de stupéfiants devra être adaptée à cet effet. Par contre, les autres demandes de renseignements, qui sortent du champ d'application de la loi susmentionnée, et qui concernent en particulier les traitements

de données personnelles effectués par les offices fédéraux, y compris les demandes relatives par exemple au système informatique provisoire de traitement des informations de protection de l'Etat ISIS, sont toujours soumises à la procédure classique du *droit d'accès direct.* Ces requêtes doivent donc être, comme par le passé, adressées directement à l'autorité concernée en vertu des dispositions de la loi fédérale sur la protection des données !

Le nouveau droit d'accès indirect fonctionne comme suit: ❶ toute personne peut exiger du préposé fédéral à la protection des données qu'il vérifie si des données la concernant sont traitées conformément au droit par un Office central. ❷ Le préposé communique alors à la personne requérante une réponse, au libellé toujours identique, selon laquelle aucune donnée la concernant n'a été traitée illégalement, ou qu'il a adressé à l'Office central la recommandation de remédier à une erreur commise dans le traitement des données. Il ne peut être fait usage d'aucune voie de droit envers cette communication. ❸ La personne concernée peut cependant exiger que la Commission fédérale de la protection des données examine la communication que le préposé a faite ou les modalités d'exécution de la recommandation qu'il a émises. ❹ La Commission fédérale de la protection des données communique à la personne concernée une réponse au libellé toujours identique selon laquelle l'examen a eu lieu conformément au sens de la requête. ❺ Enfin, les personnes recensées ayant déposé une demande d'accès sont informées conformément à la loi sur la protection des données, dès que les intérêts liés à la procédure pénale n'exigent plus le secret, mais au plus tard lors de l'expiration de l'obligation de conserver les données. Encore faut-il que cela n'entraîne pas un volume de travail excessif. Pour faciliter l'approche de cette procédure complexe, le schéma ci-dessous illustre de manière simplifiée les différentes étapes de cette nouvelle législation:

FONCTIONNEMENT DU DROIT D'ACCES INDIRECT



Remarque:

Mécanisme d'exercice du droit d'accès <u>spécifique</u> aux Offices centraux de police criminelle

Cette législation spéciale nous intègre en tant qu'autorité indépendante dans la procédure particulière du droit d'accès indirect. Les expériences étrangères dans ce domaine ont démontré l'ampleur et les difficultés inhérentes à la tâche qui nous est confiée. Nous sommes dès lors dans l'attente du personnel supplémentaire qui devra nous être attribué à cet effet.

1.2. RIPOL-4 - Les développements du système

L'Office fédéral de la police gère, en coopération avec les cantons, le système de recherche informatisé de police RIPOL. Une disposition particulière du code pénal suisse constitue la base légale formelle de ce système destiné à la recherche de personnes et d'objets. Conçu en tant que moyen informatique de diffusion des signalements, le système RIPOL a connu différents développements depuis sa mise en fonction. La dernière évolution en cours vise notamment à élaborer, au sein du RIPOL, une nouvelle banque de données pour l'ensemble des crimes et délits non élucidés ainsi que pour la recherche d'objets. Après nous avoir soumis ce projet de développement dans le cadre du concept informatique RIPOL-4, l'Office fédéral de la police nous a transmis en procédure de consultation un projet de modification de l'actuelle ordonnance RIPOL pour prise de position. Nous avons concentré notre examen sur le respect du cadre légal imposé par le code pénal et la réalisation des exigences de protection des données que nous avions fait valoir lors de l'étude du concept.

Le système informatique RIPOL est un système de recherche informatisé de personnes et d'objets qui a pour but d'assister les autorités fédérales et cantonales dans l'accomplissement de certaines tâches légales bien définies. Ces dernières sont énumérées de manière exhaustive à l'article 351bis du code pénal qui constitue la base légale formelle de ce système. Ces tâches sont notamment l'arrestation de personnes ou la recherche de leur lieu de séjour dans le cadre d'une enquête pénale ou de l'exécution d'une peine ou d'une mesure, l'internement dans le cadre de l'exécution d'une mesure tutélaire ou privative de liberté à des fins d'assistance, la recherche du lieu de séjour de personnes disparues, le contrôle des mesures d'éloignement prises à l'égard d'étrangers ou encore la recherche de véhicules et d'objets perdus et volés. Différentes autorités peuvent diffuser des signalements par le RIPOL. La loi précise également quelles sont les autorités qui peuvent obtenir des données enregistrées dans ce système.

Outre le cadre légal du système défini ci-dessus, il convient de préciser que du point de vue technique, le RIPOL a subi de nombreux développements depuis sa mise en fonction. La dernière évolution en cours vise notamment à élaborer au sein du RIPOL une nouvelle banque de données pour l'ensemble des crimes et délits non élucidés ainsi que pour la recherche d'objets. Ce concept, dénommé RIPOL-4, nous a été soumis pour prise de position. Il est le fruit des travaux de développement du système informatique entrepris par l'Office fédéral de la police. Cet office a d'ailleurs déjà fait connaître son souci de perfectionnement constant du RIPOL lors d'une journée spéciale d'information de la presse organisée par le Département fédéral de justice et police et a publié ses projets sous le titre "Perspectives d'avenir" dans une brochure explicative distribuée à cette occasion.

Les développements du RIPOL font l'objet d'une attention particulière de notre part, ce d'autant plus qu'ils impliquent certaines adaptations législatives. Ainsi, l'Office fédéral de la police, dans le cadre des travaux de modification de l'ordonnance RIPOL rendus nécessaires par l'adoption de l'article 351bis du code pénal en tant que base légale formelle du système, a également intégré dans son projet de nouvelle ordonnance des adaptations inhérentes à la mise en fonction de certains développements techniques prévus dans le concept RIPOL-4.

Selon les informations qui nous ont été fournies dans le cadre de l'examen de ce concept, il n'existe aucune banque de données uniforme au niveau national pour les crimes et délits non élucidés ainsi que pour la recherche d'objets. Ces activités ont jusqu'à présent été traitées au niveau cantonal soit par traitement électronique de données, soit par cartothèque manuelle. Seuls les crimes et délits les plus importants ou les recherches d'objets sont publiés dans le Moniteur suisse de police journalier pour assurer au moins la diffusion dans tous les cantons des cas les plus graves. L'un des objectifs visé par le concept RIPOL-4 est donc de développer le système actuel en créant une nouvelle banque de données et les applications correspondantes pour la totalité des crimes et délits non élucidés punissables selon le droit suisse, ceci combiné à la recherche d'objets. Cette extension du RIPOL permettra ainsi le démantèlement des systèmes cantonaux et assurera une saisie actualisée des données ainsi qu'une diffusion nationale de ces informations.

Le souci d'efficacité policière justifie la mise en place de ce développement qui est compatible, de notre point de vue, avec la nouvelle base légale du RIPOL. En effet, l'article 351bis du code pénal prévoit notamment que la Confédération gère en coopération avec les cantons un système de recherche informatisé de personnes et d'objets afin d'assister les autorités fédérales et cantonales dans l'accomplissement de tâches légales telles que l'arrestation de personnes ou la recherche de leur lieu de séjour dans un cadre judiciaire ainsi que la recherche de véhicules et d'objets perdus ou volés. Au cours de l'examen du projet de nouvelle ordonnance RIPOL, nous nous sommes efforcés de veiller à ce que les dispositions proposées respectent le cadre légal de l'article 351bis du code pénal. Nous avons fait de même lors de l'examen de la concrétisation juridique des développements techniques qui ont reçu notre aval.

Nous avons ainsi mis l'accent sur le caractère exhaustif de la liste légale des buts des signalements pouvant être introduits dans le RIPOL. Nous avons notamment rappelé que ce caractère exhaustif avait été à maintes reprises mis en évidence lors des débats parlementaires relatifs à l'adoption de la base légale formelle du RIPOL. Au cours de différentes observations sur le respect du cadre légal imposé par le code pénal, nous avons proposé quelques modifications de dispositions du projet d'ordonnance. Nous avons également recommandé que soient précisées certaines mesures techniques et organisationnelles relatives notamment à la journalisation, au cryptage des données, à l'utilisation des champs libres et aux autorisations d'accès.

Enfin, nous avons rappelé que d'éventuels développements modifiant la philosophie du système, telle la transformation de cette banque de données de signalements en un système permettant la comparaison et la recherche par quadrillage ("Rasterfahndung") de toutes les informations enregistrées dans les différentes banques de données du système, ne sauraient en aucun cas recevoir notre accord. De telles modifications du fondement même du RIPOL ne seraient en effet pas compatibles avec l'article 351bis du code pénal. Cette disposition a été créée pour donner une base légale formelle au système RIPOL en tant que système de diffusion des informations de recherches. Ceci a d'ailleurs été confirmé au cours des débats parlementaires. D'autre part, le Conseil fédéral s'est clairement prononcé dans le cadre du Message concernant le traitement des données en matière de poursuite pénale sur le fait que le traitement des informations policières requiert également une réglementation légale lorsque des moyens informatiques hautement

performants sont mis en oeuvre, ce qui est le cas pour le système de recherche par quadrillage.

C'est à la lumière de ces considérations que nous avons examiné le projet de développement du RIPOL prévoyant la création d'une nouvelle banque de données pour les crimes et délits non élucidés, combinée avec la recherche d'objets. Comme précisé précédemment, nous avons donné notre aval à ce développement dès lors qu'il était couvert par l'article 351bis du code pénal. Cependant, nous avons soutenu que la disposition relative à ce développement prévue dans le projet d'ordonnance pouvait, en raison de sa formulation, prêter à confusion, principalement quant au risque d'y voir une possibilité de recherche par quadrillage et de comparaison des données. Or, eu égard au caractère extrêmement sensible de ce domaine, il convient de veiller à ce que l'ordonnance RIPOL ne contienne aucune équivoque ou incertitude à ce sujet. Nous avons donc recommandé que soit expressément mentionné dans l'ordonnance qu'aucune liaison entre les banques de données du système ni procédure de recherche par quadrillage ne sont autorisées. Une telle solution, visant à obtenir une transcription juridique transparente du développement technique du RIPOL, assurerait au demeurant une meilleure sécurité du droit.

1.3. Blanchissage d'argent sale - l'avant-projet de loi fédérale

Le Département fédéral des finances a mis en consultation un avant-projet de loi sur le blanchissage d'argent dans le secteur financier. Dans le cadre de notre prise de position, nous avons principalement relevé qu'en dépit des nombreux traitements de données qu'allait impliquer l'application de cette loi, aucune réflexion relative à la protection des données n'avait été menée et qu'aucune disposition spécifique à ce sujet n'avait été introduite dans l'avant-projet.

Le 12 janvier 1994, le Conseil fédéral a autorisé le Département fédéral des finances à soumettre en procédure de consultation un avant-projet de loi fédérale sur le blanchissage d'argent dans le secteur financier (ci-après: avant-projet). Les résultats de cette procédure publiés en janvier 1995 ont démontré l'intérêt des milieux concernés pour l'instauration des devoirs d'identification et de communication du financier, mais également leurs réserves quant à l'aménagement concret de ces deux obligations. Le Conseil fédéral, ayant pris connaissance de ces résultats, a décidé que cet avant-projet devait être totalement remanié. Nous prenons acte avec satisfaction de cette décision, vu que dans le cadre de ce nouveau mandat, il pourra être tenu compte de nos remarques émises durant la procédure de consultation.

En effet, nous avons attiré l'attention de l'Administration fédérale des finances sur le fait que cet avant-projet de loi relative à la lutte contre le blanchissage d'argent allait impliquer, pour les différents organismes concernés, un important travail de traitement des données. Ce sera en particulier le cas en matière de collecte d'informations personnelles, nécessaires par exemple à la vérification de l'identité des parties. Il en ira de même de la conservation de données, tels des documents et pièces justificatives, y compris des documents d'identification, ainsi que de la mise en place de mesures organisationnelles telles que "l'établissement d'un registre central ou toute autre mesure lui permettant de fournir les données requises". Des communications et échanges de données seront finalement effectués, l'avant-projet de loi prévoyant un devoir de communication aux autorités de poursuite pénale, à

l'Office fédéral de la police ou à l'Administration fédérale des finances, ainsi que l'information de ces deux autorités par les autorités cantonales de poursuite pénale au sujet des communications leur parvenant directement.

Toutefois, aucune réflexion relative aux aspects de protection des données n'a été mentionnée dans le texte explicatif de l'avant-projet de janvier 1994, et aucune norme spécifique y relative n'a été introduite dans l'avant-projet de loi. Il est ressorti de nos investigations que la protection des données n'avait pas été abordée par le groupe de travail interdépartemental au cours des travaux d'élaboration en raison des différentes incertitudes et options encore ouvertes (par ex.: choix de l'organe de coordination et de l'organe de communication). Les implications du point de vue de la protection des données pouvant varier considérablement en fonction des choix qui seraient faits, il a alors été décidé, en accord avec l'Administration fédérale des finances, que notre prise de position se limiterait à l'établissement d'une liste provisoire des points "délicats" nécessitant une attention particulière.

Nous avons à titre préliminaire rappelé que de manière générale, dans le cadre des activités de lutte contre le blanchissage d'argent dans le secteur financier, la loi fédérale sur la protection des données est applicable tant en ce qui concerne ses principes généraux, que ses parties publique (pour l'Office fédéral de la police et l'Administration fédérale des finances) et privée (pour les banques, les fiduciaires, les gérants de fortune, les avocats indépendants, etc. ...). Elle n'étendra en revanche pas son champ d'application aux données traitées dans le cadre des procédures pénales qui seront ouvertes par les autorités de poursuites pénales compétentes. Indépendamment de l'applicabilité de la loi fédérale sur la protection des données, nous avons précisé que certaines dispositions spécifiques de protection des données devront être introduites dans l'avant-projet de loi eu égard aux nombreux traitements d'informations personnelles qu'il prévoit.

Ainsi, en ce qui concerne les durées de conservation des données par le financier, nous avons relevé que l'avant-projet de loi impose une conservation d'au moins cinq ans des documents et pièces justificatives, sous réserve des normes spéciales sur la conservation des livres. Vu que cette disposition vise également les documents d'identification, dont la durée de conservation prévue est de cinq ans au moins dès la cessation des relations d'affaires, nous avons demandé qu'une durée maximale de conservation de ces informations personnelles par le financier soit également fixée. En outre, ce devoir de conservation implique notamment l'établissement d'un registre central ou de toute autre mesure permettant de fournir les données requises. De tels registres relatifs aux clients, à leurs comptes, carnets et dépôts sont déjà tenus par les banques et autres instituts financiers. Toutefois, le devoir de communication aux autorités compétentes prévu dans l'avant-projet de loi donne naissance à toute une procédure d'échanges d'informations entre le financier, l'Office fédéral de la police, l'Administration fédérale des finances et les autorités de poursuite pénale. Il est donc probable que les informations ainsi traitées, notamment les résultats d'investigations et les décisions prises par les autorités informées, seront conservées par le financier, ce qui justifie d'autant plus la fixation d'une durée maximale de conservation de ces données dans la loi.

Afin de garantir l'efficacité des dispositions sur le devoir de communication, l'avant-projet de loi prévoit une interdiction d'informer les personnes concernées ou des tiers de la communication ou des investigations en cours pour une durée maximale de

cinq jours. Réglée au niveau d'une loi au sens formel, cette norme restrictive n'a pas suscité de remarque particulière de notre part. Par contre, nous avons recommandé que la possibilité de prolonger ce délai soit précisée et fixée pour une durée maximale déterminée.

Pour ce qui concerne le traitement des données par l'Office fédéral de la police, à savoir les données relatives au crime organisé et au blanchissage d'argent, nous avons attiré l'attention de l'Administration des finances sur plusieurs aspects problématiques du point de vue de la protection des données. Ainsi, l'avant-projet de loi définit les compétences des autorités concernées, en particulier le rôle de l'organe de coordination et les mécanismes de transmission des communications. Or, pour remplir les tâches qui lui seront confiées en tant qu'organe de coordination, l'Office fédéral de la police sera en principe amené à collecter et enregistrer les différentes communications qui lui seront parvenues, les résultats des investigations entreprises ainsi que les informations que les autorités cantonales de poursuite pénale lui auront transmises. Ce projet de loi s'incrivant dans la même perpective que la loi sur les offices centraux de police criminelle de la Confédération, il conviendra de déterminer si ces informations seront gérées par les offices centraux de l'OFP dans le même cadre de traitement de données que celui prévu par la loi fédérale sur les Offices centraux de police criminelle ou au contraire de manière totalement séparée. De la solution choisie dépendra la nécessité de prévoir dans l'avant-projet un renvoi à la loi sur les Offices centraux ou l'élaboration d'une disposition spécifique de traitement des données relatives au blanchissage d'argent dans le secteur financier. En outre, si l'Office fédéral de la police traite ensemble les données relatives au crime organisé et les informations concernant le blanchissage d'argent, il conviendra d'en tenir compte, tant pour la communication de données que pour les droits d'accès. En effet, l'Administration fédérale des finances ne devra avoir accès qu'au second groupe de données citées.

Nous avons également relevé que le choix de l'organe de coordination aura des conséquences sur le contenu des règles de protection des données à élaborer. L'attribution de cette tâche à l'Office fédéral de la police nécessiterait, comme relevé ci-dessus, des précisions quant aux traitements de données relatifs au crime organisé et au blanchissage d'argent. La désignation éventuelle de l'Administration fédérale des finances requerrait également l'élaboration de règles spécifiques, concernant notamment les informations amenées à transiter par cet office et la gestion probable d'une banque de données spécifique au blanchissage d'argent. L'avant-projet de loi prévoit en effet que l'Office fédéral de la police devra fournir à l'Administration fédérale des finances toutes les données et informations nécessaires.

Les modes de transmission de données et les accès à ces dernières ont suscité de notre part de nombreuses remarques. Ainsi, il conviendra de réglementer l'étendue desdits accès en fonction des choix opérés pour le traitement des informations collectées et échangées dans le cadre de l'application de la future loi. En effet diverses dispositions de l'avant-projet impliquent, entre les organes concernés, la transmission de communications, la fourniture d'informations et l'annonce de décisions telles que le blocage d'une transaction, une décision pénale ou une ordonnance de non-lieu. Le commentaire explicatif soutient notamment que l'Office fédéral de la police et l'Administration fédérale des finances "devront de toute façon collaborer étroitement". Or, aucune précision n'est apportée quant aux modes

possibles de transmission des données qui sont envisagés. Nous avons donc attiré l'attention de l'Administration fédérale des finances sur le fait que si certains accès aux informations détenues par l'organe de coordination ou certains échanges de données personnelles entre l'Office fédéral de la police et l'Administration fédérale des finances sont envisagés sous forme de procédure d'appel (liaisons online), une réglementation spécifique dans la loi devra expressément le prévoir.

Enfin, nous avons insisté sur le fait que si, comme relevé précédemment, les normes de protection des données n'ont pas d'effet dans le cadre d'enquêtes pénales en cours, la bonne application de cette loi dépendra cependant d'une étroite collaboration entre l'Office fédéral de la police, l'Administration fédérale des finances et les autorités cantonales de poursuites pénales. Or certaines informations identiques seront soumises à des régimes juridiques différents selon l'autorité qui les traitera. Ainsi, les dispositions de procédure du droit cantonal s'appliqueront à une procédure pénale en cours. Ces normes régleront notamment les droits des personnes concernées (droit de consultation) et le traitement des données par le juge d'instruction. Par contre, qu'en sera-t-il des mêmes données, en mains de l'organe de coordination? Nous avons donc demandé à ce que soient par exemple réglés spécifiquement tant la durée de conservation des informations détenues par l'organe de coordination que le droit de consultation des personnes concernées à ces données. Ces mêmes points devront aussi être réglés si l'Administration fédérale des finances traite certaines données en tant qu'organe de communication. Il conviendra enfin de déterminer si les communications fondées sur des soupçons pourront être conservées, et si oui, pour combien de temps, par les organes de coordination et/ou de communication, dans les cas où aucune enquête n'est finalement ouverte par l'autorité pénale compétente.

Dans le cadre de la publication des résultats de la procédure de consultation, le Département fédéral des finances a informé le Conseil fédéral de nos observations en attirant son attention sur le fait que la collecte, la conservation et la communication de données effectuées en application de cette nouvelle législation devront être étudiées à la lumière de la loi fédérale sur la protection des données. Nous saluons cette démarche. Durant les travaux de remaniement de l'avant-projet demandés par le Conseil fédéral, il conviendra dès lors que soient prises en compte nos différentes observations et que des dispositions claires de protection des données soient élaborées.

1.4. Révision de l'ordonnance sur le casier judiciaire

En même temps que la LPD est entré en vigueur un article du Code pénal statuant que les demandes d'extrait de casier judiciaire émanant d'autorités pénales effectuées auprès du Bureau central suisse de police (BCP) sont enregistrées pendant une durée maximale de 2 ans. Cette disposition prévoit en outre que le BCP est en droit de communiquer à l'autorité pénale requérante auprès de quelle autre autorité pénale une procédure a été engagée.

Le BCP enregistre pendant deux ans les demandes d'extraits de casier judiciaire reçues de la part d'autorités pénales de la Confédération ou des cantons en rapport avec des procédures en cours. Les données suivantes sont saisies: l'autorité requérante, l'identité de la personne inculpée, le motif d'inculpation ainsi que la date

à laquelle l'extrait du casier judiciaire a été délivré. Si une autorité pénale demande un extrait de casier judiciaire dans le cadre d'une procédure pénale, le BCP communique les données correspondantes à l'autorité pénale. L'autorité pénale communique au BCP les acquittements et les arrêts de non-lieu prononcés dans des procédures pour lesquelles un extrait de casier judiciaire avait été demandé, après quoi le BCP détruit les données enregistrées. Les détails, tels que la responsabilité du traitement des données, les droits de procédure de la personne concernée, la collaboration avec les cantons et les autorités qui sont compétents pour le droit de consultation des données ainsi que pour leur rectification et destruction, doivent être réglés dans une ordonnance. C'est pour cela que l'ordonnance sur le casier judiciaire doit être révisée. Le projet, auquel nous avons contribué, se trouve en ce moment auprès de l'Office fédéral de la police avec lequel une bonne collaboration a été possible.

2. Droit des étrangers et droit d'asile

2.1. Registre central des étrangers RCE

En règle générale, il est interdit de consulter, dans le Registre central des étrangers (RCE) les données de personnes non recherchées (tiers non concernés) pour les communiquer et, en aucun cas, pour les traiter ultérieurement.

L'an passé, nous avons recommandé au maître du fichier RCE, l'Office fédéral des étrangers, de ne pas communiquer à l'Office fédéral de la police, par procédure d'appel (principe du self-service) ou en grand nombre, les données des quelque 3,5 mio d'étrangers recensées dans le RCE (voir notre 1er rapport d'activités p. 108 ss). Nous estimions suffisante la communication sur demande et de cas en cas, en raison notamment de l'accès élargi dont bénéficient toutes les autorités de police et l'Office fédéral de la police aux fichiers élaborés spécialement pour la recherche et aux autres secteurs de la police, dans lesquels figurent des criminels, dont des étrangers. Le RCE n'est pas une banque de données de recherche judiciaire. Avec les moyens usuels de la bureautique, il est de surcroît possible de relier ou de comparer entre eux tout ou partie des différents fichiers disponibles (recherche par quadrillage). Cette procédure est juridiquement inadmissible, raison pour laquelle il faut également choisir, au niveau de l'organisation du système, une solution qui, d'emblée, ne permette que des traitements de données autorisés (pas d'accès préalable simultané au RCE et aux cartothèques de recherche du secteur de la police).

Lors de la révision de l'ordonnance sur le RCE, le Conseil fédéral et le Département fédéral de justice et police ont décidé que la police pouvait continuer à accéder au RCE par procédure d'appel, tout en respectant certaines restrictions et charges:
tout d'abord, les consultations ne sont autorisées que pour l'identification de personnes, avec un accès limité uniquement à quelques champs de données. Elles doivent être consignées dans un protocole, lui-même soumis à des contrôles réguliers. En principe, le traitement de données de personnes non recherchées est interdit, de même que la recherche par quadrillage. L'Office fédéral des étrangers est tenu, en collaboration avec l'Office fédéral de l'informatique, de vérifier la sécurité et l'organisation lors du traitement des données du RCE. L'Office fédéral de la police,

pour sa part, doit compléter l'analyse des tâches des services qui consultent les données du RCE.

Certes, sous l'angle du droit de la police et des étrangers, les autorités compétentes ont pondéré autrement la protection de la personnalité, mais elles ont suivi nos propositions pour les questions importantes qui se posent au sujet des mesures de protection nécessaires au traitement de données.

La révision de l'ordonnance sur le RCE a soulevé, outre la question de l'accès online par les autorités de police, d'autres questions relatives à la protection des données:

- nous avons défendu le point de vue selon lequel la modification ou l'extension importantes d'un grand système TED sont soumises, comme le RCE, aux prescriptions de la LPD ou de l'OLPD, sans être tributaires du délai transitoire de l'article 38 LPD. D'où la nécessité d'avoir une base légale dans une loi au sens formel pour la nouvelle installation de raccordements online permettant aux autorités de police de consulter également des données sensibles.
- Nous n'avons pas non plus réussi à faire passer notre suggestion de régler l'admissibilité de la communication de données de l'asile par l'Office fédéral des réfugiés au RCE pour l'établissement des passeports de réfugiés, non pas dans l'art. 5, al. 1, lettre b, mais dans les dispositions transitoires de l'ordonnance sur le RCE. Un tel échange de données établi sur la durée aboutit en effet, quant à son résultat, à une banque de données commune, inadmissible sous l'angle de la protection des données. Dès que l'Office fédéral des réfugiés sera en mesure d'imprimer lui-même les passeports des réfugiés, l'article 5, 1er alinéa, lettre b de l'ordonnance sur le RCE devra être supprimé.

Communication de données du RCE à des autorités non reliées au RCE
Une autorité cantonale de police des étrangers nous a demandé s'il était possible de communiquer en grand nombre à des autorités communales ou cantonales non reliées au RCE, au moyen de "listes électroniques", des données concernant les étrangers. Nous avons relevé que selon l'ordonnance sur le RCE, plusieurs autorités communales et cantonales clairement définies dans le RCE avaient le droit de disposer du RCE et ainsi d'accéder, par procédure d'appel, aux données dont ils avaient besoin. De plus, le RCE offre à ces autorités de nombreuses fonctions techniques d'assistance, notamment la possibilité de rechercher des personnes et des dossiers ou de procéder à un contrôle de gestion. Ainsi, les autorités citées dans l'ordonnance sur le RCE ont à leur disposition un instrument électronique de travail moderne. Les possibilités multiples et variées de traitement de données imposent de ce fait une protection des données développée en conséquence, à l'instar de ce qui a été réalisé dans le RCE au moyen de mesures comparativement tout aussi importantes. Si, comme demandé, on devait tirer du système un grand nombre de données relatives à des étrangers pour les remettre à des autorités non mentionnées dans l'ordonnance sur le RCE, tant les prescriptions de protection des données contenues dans cette ordonnance que celles de la LPD seraient violées; d'où le caractère inadmissible d'une telle communication de données.

Suisses et Suissesses dans le Registre central des étrangers
Des personnes privées ont à maintes reprises attiré notre attention sur le fait que des Suisses figuraient également dans le RCE et que la police pouvait, le cas

échéant, consulter leurs données grâce à son système de recherche automatisée (RIPOL). L'ordonnance sur le RCE prévoit dans différents articles le traitement de données relatives à des Suisses:

- ainsi, par exemple, les données des personnes naturalisées en Suisse sont, d'après l'ordonnance sur le RCE, effacées du RCE après deux ans.
- Les autorités cantonales et communales du marché du travail annoncent en permanence au RCE les adresses des employeurs qui sollicitent une autorisation.
- L'Office fédéral des étrangers récolte en outre les lettres d'invitation d'hôteliers et restaurateurs suisses à des étrangers.
- En outre, les autorités de police ont connaissance des données nécessaires aux contrôles de police des étrangers et à l'identification des personnes; d'après la teneur de l'ordonnance, il est possible, au besoin, de compléter ces données par l'adresse qui, dans certains cas, peut également se référer à un Suisse ou à une Suissesse.

Pour le reste, l'ordonnance sur le RCE ne donne aucune indication sur les données des Suisses et Suissesses figurant dans le RCE. C'est pourquoi nous pensons qu'il n'est pas possible de déduire de ces dispositions une quelconque autorisation de communiquer aux autorités de police les noms des hôtes suisses. Quant à la question légitime de savoir si les noms des hôtes suisses peuvent (et doivent) figurer dans le RCE, elle est en cours d'éclaircissement.

2.2. Système de gestion sans papier des dossiers de personnes (REGI-2)

Dans la mesure du possible, il faut concevoir les grands systèmes TED de sorte à exclure d'emblée les traitements illicites de données. Les "dossiers électroniques" doivent être élaborés de manière à offrir différents niveaux d'accès selon les tâches. L'Office fédéral des étrangers s'est déclaré d'accord avec notre recommandation.

Les questions de la conception ou de l'architecture des grands systèmes TED se sont également posées dans le cas du système de gestion sans papier des dossiers de personnes REGI-2 de l'Office fédéral des étrangers (voir aussi notre 1er rapport d'activités, p. 109). Etant donné qu'un système TED permet à une foule d'utilisateurs de traiter de grandes quantités de données, il est impératif de prendre en compte minutieusement les aspects de la protection des données déjà au moment du développement. Il s'agit essentiellement, lors de la conception concrète du système en question, de créer les conditions pour que les utilisateurs du système se comportent conformément au droit de la protection des données dans le cadre de leur travail. Le système doit par conséquent d'emblée être conçu de manière à ne permettre que des traitements de données conformes au droit. Dans le cas particulier, il faut veiller à effectuer une analyse des tâches auprès des utilisateurs ou unités d'organisation d'utilisateurs. Dans ce contexte, les questions suivantes se posent:

- le traitement de données personnelles avec des moyens électroniques dans un contexte précis est-il réellement nécessaire et est-il légalement autorisé?
- Dans ce cadre, faut-il traiter des données sensibles ou des profils de la personnalité?
- Les données doivent-elles être régulièrement communiquées à des tiers? Existe-t-il des intérêts légitimes contraires et comment faut-il les évaluer?
- Comment peut-on protéger efficacement les données contre la perte, les modifications ou le traitement non autorisés
- Comment peut-on notamment empêcher des détournements du principe de finalité, lorsque, par exemple, il existe déjà une autorisation d'accès à différents autres fichiers électroniques?

Toutes ces questions n'avaient pas encore été totalement élucidées et la documentation exigée par l'ordonnance sur la protection des données faisait elle aussi défaut. Il n'était notamment pas clair de savoir comment garantir, entre autres, dans le cas de dossiers volumineux, uniquement la communication des données vraiment nécessaires au destinataire, tout en respectant les principes de finalité et de proportionnalité. Il a également été prévu de procéder à de vastes traitements de données en vue de REGI-2 (lecture ou scanérisation de la totalité des dossiers de l'OFE sur un seul support de données). C'est pourquoi nous avons recommandé de suspendre le traitement des données pour le REGI-2 jusqu'à ce que les questions encore ouvertes soient résolues et que les résultats soient juridiquement satisfaisants. L'OFE a accepté notre recommandation et présenté à la fin 1994 un règlement de traitement dont il reste maintenant à examiner la conformité avec la protection des données.

2.3. Registre automatisé des personnes AUPER-2

La police doit aussi pouvoir accéder aux données sur l'asile inscrites dans le Registre automatisé des personnes AUPER-2 de l'Office fédéral des réfugiés (ODR). Lors d'une révision partielle de l'ordonnance AUPER et malgré notre recommandation, le Conseil fédéral et le Département fédéral de justice et police (DFJP) ne se sont malheureusement pas (encore) exprimés en faveur d'une protection des droits des tiers non concernés. C'est pourquoi un examen de l'AUPER a été ordonné; il est actuellement en cours.

L'année dernière, nous avons recommandé que les données des requérants d'asile et des réfugiés inscrites dans l'AUPER ne puissent pas être communiquées par procédure d'appel ou en grand nombre à l'Office fédéral de la police (OFP), par exemple. A notre avis, une communication sur demande et de cas en cas par l'ODR, maître du fichier, des données relatives à l'asile enregistrées dans l'AUPER était suffisante. (Voir également notre 1er rapport d'activités, pp. 107 et 108).

En novembre de l'année dernière, le DFJP a autorisé l'OFP à poursuivre provisoirement le traitement des données de l'AUPER relatives aux requérants d'asile et aux réfugiés, tout en maintenant l'interdiction de l'assemblage systématique des données avec d'autres banques de données ou la recherche par quadrillage et en respectant toujours les interdictions de communiquer à l'étranger les données relatives à l'asile régies par le droit national et le droit international public. Simultanément, le DFJP a attiré l'attention sur la nécessité d'une vaste analyse d'organisation et de sécurité, telle que décidée par l'ODR il y a peu, et exigé que ses résultats soient transposés dans une réglementation définitive d'accès dans le cadre de la prochaine révision totale de l'ordonnance AUPER. Actuellement, une séparation d'AUPER en un secteur "asile" et un secteur "police" est à l'examen.

Lors d'une révision partielle de l'ordonnance AUPER, le Conseil fédéral a par ailleurs accordé aux autorités cantonales de police et aux postes-frontières un accès online aux données d'AUPER sur l'asile. Malgré nos demandes, on a renoncé, comme dans le reste du secteur de l'asile, à édicter des prescriptions de protection adéquate, notamment des droits des tiers non concernés (communication limitée des données lors des procédures de recherche, interdiction d'un traitement ultérieur, journalisation de la consultation des données). Vu les développements actuellement en cours dans le secteur de l'informatique et vu les situations de dangers particulières que les personnes poursuivies connaissent dans leur patrie, cette décision est fort regrettable du point de vue du droit de la protection des données. Ce d'autant plus qu'il faut aussi communiquer la nationalité de manière non contrôlée au moyen de la procédure d'appel et ce sans mesures de protection. Par ce biais, les personnes concernées sont exposées inutilement à une source possible de danger supplémentaire et l'on donne ainsi en même temps des indications indirectes sur l'appartenance à une race, élément qui fait partie des données sensibles. Il reste à espérer que le Conseil fédéral reviendra sur sa décision lors de la prochaine révision de l'ordonnance AUPER.

Lors de la révision partielle susmentionnée, les bases pour une gestion externe du compte de sécurité des requérants d'asile - point d'ailleurs réglé dans la loi sur l'asile et l'ordonnance 2 sur l'asile - ont été élaborées. Nous avons accepté sous des conditions strictes l'échange prévu d'informations dans le secteur des PTT, avec la

promesse qu'elles seraient respectées au moment opportun. Malheureusement cela ne s'est pas produit jusqu'à présent et nous avons émis une recommandation conjointement à l'Office fédéral de l'informatique. Conformément à ce qui précède, il faudra élaborer entre les nombreux organes impliqués un concept global de sécurité assorti d'un catalogue de mesures appropriées. Les échanges de données doivent être systématiquement chiffrés. Dans le secteur des PTT, le compte lui-même doit être complètement séparé des autres traitements de données. Il faut élaborer un règlement de traitement au sens de l'ordonnance sur la protection des données. Dans le cadre de cette révision partielle, nous avons finalement demandé en vain de renoncer à un échange de données entre l'AUPER et le RCE, un tel échange étant contraire aux principes de traitement du droit de la protection des données.

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

Les accès directs à des fin d'entraide administrative aux banques de données des étrangers et de l'asile doivent être limités, et il faut protéger correctement les données des tiers non concernés contre des "actions de recherche" etc. non autorisées. Les communications de données à l'étranger ne doivent se faire que dans des cas particuliers et après une pesée des intérêts. Quant aux empreintes digitales, elles ne peuvent être prélevées que dans une mesure raisonnable.

Nous avons déjà donné un aperçu, dans notre 1er rapport d'activités (voir p. 110 à 112), des questions de protection des données qui se poseront lors de la révision de la loi sur les étrangers et de la loi sur l'asile. En résumé, nous pouvons aujourd'hui également évoquer les points suivants:

- si des données relatives à des étrangers et des requérants d'asile doivent être rendues accessibles aux autorités de police, par exemple par procédure d'appel, il faut que l'ampleur et le but de ces accès soient décrits avec suffisamment de clarté dans la base légale correspondante.
- Si le RCE ou l'AUPER sont les seules possibilités modernes d'identification rapide d'un étranger ou d'un requérant d'asile, ce but doit ressortir du texte de la loi.
- Simultanément, la loi doit aussi contenir l'interdiction de communiquer en règle générale et, dans tous les cas, de traiter ultérieurement les données d'autres personnes ne devant pas être identifiées (tiers non concernés). En outre, la loi doit mentionner dans les grandes lignes les mesures de protection y relatives, tel le contrôle des interrogations des systèmes.
- Dans le domaine délicat de l'asile notamment, les communications de données à l'étranger ne doivent être autorisées que de cas en cas et après une pesée des intérêts, car dans le cas contraire, le respect de l'interdiction de transmission prévu dans le droit national et le droit international public serait violé. Les dérogations à ce principe, dans le but de déterminer plus rapidement la compétence pour le traitement d'une demande d'asile dans l'espace européen, doivent être formellement inscrites dans la loi lorsqu'elles s'avèrent nécessaires.
- Le prélèvement et la transmission des empreintes digitales d'étrangers ou de requérants d'asile non criminels ne doivent entrer en ligne de compte qu'en dernier ressort. A nos yeux, il est indiscutablement anticonstitutionnel et contraire au droit d'adopter dans une base légale une prescription qui oblige à

prélever sans exception les empreintes digitales de tous les requérants d'asile, y compris les enfants et les personnes âgées. Si des empreintes digitales sont prélevées, elles doivent être conservées et traitées séparément des données relatives aux criminels.

Traités internationaux
Après les deux accords avec l'Allemagne et la Hongrie concernant la reprise de personnes à la frontière (voir notre 1er rapport d'activités, pp. 112 et 113), un traité a été conclu sur la même base durant cet exercice avec la Roumanie et la Bulgarie. Ainsi, s'agissant de l'exécution de ce traité, seules les données mentionnées dans le catalogue des données peuvent être transmises également aux autorités désignées avec précision dans l'accord. Les éventuelles interdictions de transmission qui ressortent du droit national ou de traités qui ont la primauté demeurent réservées.

Un autre accord avec l'Allemagne doit permettre, à des fins de statistique, une comparaison unique des empreintes digitales d'un certain nombre de requérants d'asile accueillis dans les deux Etats du traité. Nous avons demandé des indications et des documents détaillés afin d'avoir une appréciation fondée du projet du point de vue du droit de la protection des données.

3. Télécommunications

3.1. RNIS / SwissNet 2

Le réseau de communication digital SwissNet offre une multitude de fonctions utiles à ses utilisateurs/utilisatrices. Du point de vue de la protection des données, il importe cependant d'apporter certaines réserves, surtout en ce qui concerne la transmission des numéros d'abonné.

En octobre 1992, les Télécom PTT ont commencé l'exploitation du réseau numérique à intégration de services (RNIS) suisse, appelé «SwissNet 2». Il s'agit là d'un réseau de télécommunication numérique permettant de transmettre autant la voix que les données, le téléfax et l'image. On peut s'abonner à SwissNet au moyen d'un raccordement primaire (30 canaux de transmission à 64 kbit/s chacun) ou d'un raccordement de base (2 canaux de transmission à 64 kbit/s chacun). Le raccordement de base peut déjà présenter un intérêt pour de petites entreprises ou pour des utilisateurs privés. RNIS offre beaucoup d'avantages aux utilisateurs: ils sont plus faciles à atteindre, bénéficient de taux de transfert plus élevés, d'une utilisation plus aisée; bref le confort a été amélioré et les communications deviennent plus efficaces.

Le réseau numérique permet également de saisir et d'enregistrer un grand nombre de données relatives à la communication, ce qui pose des problèmes du point de vue de la protection des données. Sur la base de l'identification de l'appelant (Calling Line Identification Presentation, CLIP), l'abonné SwissNet voit sur l'affichage de son appareil téléphonique le numéro de l'appelant *avant* qu'il décroche pour répondre à l'appel. En Suisse, un abonné SwissNet voit les numéros des personnes l'appelant même si celles-ci ne sont pas des abonnés SwissNet, il suffit qu'elle soient reliées à un central numérique, ce qui est actuellement le cas pour la majorité des

raccordements téléphoniques. Il suffit donc à l'appelé d'avoir un accès direct à un annuaire électronique pour qu'il soit en mesure d'obtenir immédiatement le nom et l'adresse de l'appelant. Ceci lui permet de distinguer les appels importants de ceux qui le sont moins, mais aussi d'identifier les appelants qui pourraient l'importuner. L'appelant, de son côté, est en mesure de s'identifier grâce à la transmission de son numéro d'abonné.

Il existe cependant certains cas dans lesquels il n'est pas souhaitable que l'appelant soit identifié. Prenons comme exemple les services d'assistance anonyme (par ex. dans le domaine médical) ou la possibilité de ne pas répondre aux appels de certaines personnes. Ce qui pose également problème est que l'accès aux données d'identification n'est pas toujours limité à la personne appelée (par ex. lorsqu'un raccordement est utilisé par plusieurs personnes).

En principe, chaque abonné doit avoir la liberté de décider lui-même si son numéro d'appel est transmis à d'autres abonnés. La solution idéale consisterait à pouvoir supprimer la transmission du numéro de manière individuelle, c.-à-d. que l'appelant décide à chaque appel qu'il fait, s'il veut que son numéro d'abonné soit transmis ou non. L'appelé est également libre de décider s'il veut répondre à l'appel. Les abonnés qui désirent que leur numéro de téléphone ne soit pas visible sur l'appareil téléphonique d'un abonné SwissNet, peuvent actuellement demander la suppression de manière générale de la transmission du numéro (contre paiement d'une taxe unique et d'une surtaxe mensuelle).

Les Télécom PTT réalisent le RNIS par étapes. Le système actuellement en service (SwissNet 2) ne permet pas encore la suppression individuelle de la transmission du numéro d'abonné. L'étape suivante (SwissNet 3) offrira cependant cette possibilité, mais seulement aux abonnés SwissNet. Selon les Télécom PTT, la suppression individuelle du numéro de téléphone pour les abonnés disposant d'un raccordement analogique ne sera pas réalisée pour des raisons techniques et pratiques, bien qu'il ne soit pas exclu que cela soit faisable.

Sur la base des faits communiqués, nous avons transmis les propositions d'amélioration suivantes aux Télécom PTT:

- tous les abonnés au téléphone doivent être informés par écrit que leur numéro de téléphone peut être affiché sur l'appareil d'un abonné SwissNet. Ils doivent également apprendre qu'ils ont la possibilité de faire supprimer cette transmission de manière générale. Cette information doit être faite de manière à ce que l'on puisse ensuite présumer que les clients connaissent cet état de fait. Dans la situation actuelle, on ne peut absolument pas admettre que les abonnés au téléphone soient conscient du fait que leur numéro de téléphone est visible pour tous les abonnés SwissNet.
- Afin que le client puisse vraiment décider librement, nous sommes d'avis que la suppression du numéro de l'appelant ne doit pas - contrairement à la pratique actuelle - être facturée sous forme de prestation supplémentaire. La seule solution acceptable serait un modeste émolument unique pour effectuer la modification.
- L'appelant devrait être en mesure de savoir si le numéro qu'il appelle est un raccordement SwissNet, donc s'il est possible que son numéro soit transmis.

Les annuaires téléphoniques auxquels les clients ont actuellement accès n'indiquent pas cet état de fait.

En plus de la transmission automatique du numéro de téléphone, il existe d'autres fonctions mises en oeuvre surtout dans les installations RNIS et problématiques du point de vue de la protection des données:

- dispositif mains libres: l'appareil de téléphone est équipé d'un haut-parleur et d'un microphone incorporés permettant de téléphoner les mains libres. Cela signifie cependant que la conversation peut également être entendue par d'autres personnes qui se trouvent dans la même pièce, sans que l'appelant en soit forcément conscient.
- Appel direct: cette fonction permet à *l'appelant* d'activer le haut-parleur et le microphone de l'appareil de l'appelé afin de pouvoir immédiatement lui adresser la parole. De telles installations permettent également de procéder à une écoute des bruits présents dans une pièce. Afin de prévenir les abus, un voyant sur l'appareil de téléphone doit clairement indiquer si le microphone est enclenché ou non.

3.2. Internet

Internet représente le réseau informatique le plus grand qui soit au monde. Il s'agit plus précisément d'une mise sur réseau d'un grand nombre de réseaux individuels et contenant un volume absolument gigantesque d'informations. Ces derniers temps, le nombre d'utilisateurs d'Internet est en très forte croissance, ce qui nous amène à porter certaines réflexions du point de vue de la protection des données.

Le précurseur d'Internet était un réseau militaire américain conçu de manière aussi décentralisée que possible afin de pouvoir rester opérationnel même en cas de panne partielle. Plus tard, ce réseau fut étendu, surtout au domaine scientifique universitaire. Depuis un certain temps, de plus en plus d'entreprises et de personnes privées profitent de la pléthore d'informations disponibles sur ce réseau et mettent elles-mêmes des informations à disposition. L'utilisateur d'Internet peut utiliser les fonctions les plus variées: il peut envoyer et recevoir du courrier électronique, participer à des forums thématiques publics (appelés Newsgroups), télécharger des fichiers depuis un ordinateur ou travailler depuis son écran sur un autre ordinateur du réseau Internet comme s'il se trouvait sur place. Il existe d'autre part des interfaces d'interrogation conviviales telles que le "World Wide Web", permettant d'accéder aisément à ce volume d'informations démesuré. Internet a énormément gagné en popularité ces derniers temps; le nombre d'utilisateurs actuel est estimé entre 30 et 40 millions et il ne semble pas que cet engouement s'apaise prochainement.

Du point de vue de la protection des données, Internet soulève des objections majeures:

- il ne dispose pas d'un ordinateur central. Il n'existe pas non plus d'instance centrale veillant à éviter les violations de la protection des données. De fait, toute personne est libre de faire ce qu'elle veut au sein d'Internet. C'est la raison pour laquelle ce réseau donne l'impression d'être un ensemble plutôt

chaotique. Il semble que personne n'ait vraiment une vue d'ensemble sur la situation d'Internet.

- Outre l'absence d'instance de contrôle centrale neutre, le manque de dispositions communes de protection des données au niveau international ou même mondial, capables d'assurer la protection transfrontière des données d'Internet est problématique. Actuellement, ce sont très vraisemblablement les dispositions sur la protection des données du pays à partir duquel les données sont envoyées ou mises à disposition pour consultation qui font foi.
- Une grande partie des informations disponibles sur Internet est prévue pour être consultée par n'importe qui. Il faut veiller dans ce contexte à ce que les données mises à disposition ne soient pas des données personnelles en soi anodines, mais qui peuvent, en connexion avec d'autres données librement consultables, constituer des profils de la personnalité. Des données prévues pour une consultation libre ne sont pas confidentielles. Le problème de la confidentialité se présente cependant lorsque des messages personnels ou des données non prévues pour le public sont transmises à travers le réseau. Il n'existe pas de mesures standard pouvant garantir la confidentialité. Un message transmis par Internet peut être lu par un grand nombre de personnes au cours de son trajet de l'expéditeur au destinataire.
- Un autre problème qui se pose est celui de la vérification de l'identité du partenaire avec lequel on communique. Le destinataire d'une information ne peut jamais avoir la certitude que l'expéditeur est vraiment la personne qu'il prétend être, étant donné qu'Internet ne connaît pas de mécanisme permettant d'authentifier l'identité d'un correspondant.
- En enregistrant, puis en analysant les rapports de communication (par exemple au niveau du courrier électronique) il est possible de constituer des profils de communication. En d'autres mots, il est possible de constater quels sont les partenaires avec lesquels une personne donnée échange des communications, quand et à quelle fréquence.
  Des données personnelles peuvent également résulter de l'utilisation d'informations librement accessibles (pages d'information, banques de données, fichiers publics, etc.). Les problèmes soulevés sont comparables à ceux que nous avons évoqués en rapport avec la télévision interactive (voir p. 131). Indépendamment de l'enregistrement des données consultées, on peut, simplement en recensant les heures pendant lesquelles un utilisateur est connecté au réseau, tirer des conclusions sur le comportement de l'utilisateur à son bureau (ou dans ses loisirs, en cas d'utilisation à titre privé).
- Internet comprend plusieurs milliers de "Newsgroups" traitant les thèmes les plus variés. Ainsi est-il relativement facile, à l'aide de simples programmes, d'examiner systématiquement les articles rédigés par une personne donnée par la présence de certains mots clés. Un tel procédé permettrait alors d'obtenir par exemple une image très détaillée des opinions, intérêts et activités des personnes qui rédigent des articles pour les "Newsgroups". Une utilisation abusive facile à concevoir consiste à utiliser les données pour des envois publicitaires ciblés. En ce qui concerne les possibilités d'utilisation, la fantaisie ne connaît pas de limites.

Un certain nombre de risques peuvent être limités par les utilisateurs eux-mêmes grâce à des mesures techniques et organisationnelles. Ils peuvent par exemple chiffrer les informations confidentielles ou améliorer l'authenticité de documents à l'aide de systèmes électroniques de signature. Des réseaux d'entreprise désirant

communiquer par Internet peuvent être isolés à l'aide d'ordinateurs frontaux intermédiaires pour prévenir d'éventuelles intrusions en provenance d'Internet. Il est important que toute personne accédant à Internet soit consciente des risques et périls qu'elle encourt. Quiconque transmet des messages non cryptés doit s'attendre à ce qu'ils soient lus par des tierces personnes. (En ce qui concerne la problèmatique des personnes mettant à disposition pour consultation dans les annuaires électroniques des données concernant d'autres personnes, voir également le chiffre 3.3 ci-dessous).

Étant donné que le réseau Internet échange ou met à disposition des données au niveau international et mondial, il incombe de rendre attentif au fait que les législations en matière de protection des données dans les pays vers lesquels les données sont envoyées sont très disparates. Conformément à la LPD, des données ne peuvent pas être communiquées à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée. Cela est notamment le cas lorsqu'il n'y a pas de protection des données équivalente à celle de la Suisse. La plupart des problèmes mentionnés n'existent pas seulement dans le réseau Internet, mais également avec d'autres messageries commerciales (telles que CompuServe par exemple) ou avec les réseaux de messageries, qui disposent en outre très souvent de passerelles vers Internet.

3.3. Annuaires électroniques

Lorsque des données personnelles sont mises à disposition sur des réseaux électroniques nationaux, internationaux ou mondiaux par des personnes autres que les personnes concernées elles-mêmes, la disponibilité et la connectabilité des données ainsi que le manque de contrôle de ce qu'il advient de ces informations pose un gros problème.

L'utilisation de l'informatique progresse sans cesse. Exemple: les annuaires électroniques, qui contiennent de plus en plus souvent des données personnelles. Parfois, ces annuaires se trouvent dans des réseaux fermés, l'accès aux données étant ainsi limité à un cercle déterminé de personnes. Une grande partie de ces annuaires est par contre disponible dans des réseaux publics, ce qui signifie que les données qui y sont enregistrées peuvent être accessibles à n'importe quelle personne au plan national, international ou même mondial. Du point de vue de la protection des données, nous devons distinguer entre de tels traitements de données et ceux qui sont effectués par l'employeur.

En général
Quiconque met à disposition, par le biais de lignes de télécommunication, des données personnelles accessibles par procédure d'appel est lié par les principes de la protection des données. Ces principes sont applicables tant à des informations relatives aux qualifications, spécialisations, passe-temps, mensurations, etc. d'une personne identifiée ou identifiable qu'aux données telles que le nom, l'adresse, le numéro de téléphone, le numéro de fax, l'adresse pour le courrier électronique et d'autres paramètres de communication. Plus les données traitées sont sensibles, plus les exigences en matière de protection des données sont élevées. Quiconque rend accessibles des données relatives à d'autres personnes est également tenu de veiller à la sécurité de ces données, notamment à leur confidentialité, disponibilité et

exactitude. Pour le cas où les données sont rendues accessibles sur un plan international, voire mondial, il y a lieu de veiller à ce qu'elles ne soient pas communiquées à l'étranger au cas où la personnalité des personnes concernées devait s'en trouver gravement menacée. Ceci est notamment le cas lorsque le pays en question ne connaît pas de législation en matière de protection des données équivalente à la nôtre. Les lois de protection des données manquantes peuvent être remplacées par des dispositions contractuelles.

Lorsque des personnes privées mettent à disposition des informations relatives à d'autres personnes dans des réseaux électroniques nationaux, internationaux ou mondiaux, ceci devrait nécessiter l'approbation écrite des personnes concernées. Cet accord devrait idéalement englober la prise de connaissance:

- des données traitées,
- du réseau dans lequel les données sont disponibles,
- du but du traitement dans le réseau,
- des possibilités et des risques inhérents au réseau (disponibilité, connectabilité),
- d'une éventuelle disponibilité à l'échelle mondiale,
- du défaut éventuel de législation de protection des données adéquate dans certains pays dans lesquels l'accès aux données est possible.

Les personnes concernées devraient avoir le droit de déterminer elles-mêmes les données saisies et de retirer leur consentement.
Une déclaration de consentement pourrait être rédigée comme suit:

PROPOSITION

DÉCLARATION DE CONSENTEMENT

Nom: _____ Prénom: _____
Adresse: _____

Je déclare par la présente accepter que mes données personnelles suivantes

[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]

soient mises à disposition
sur le système _____ de l'entreprise/organisation _____.
Le but du fichier consiste à _____
_____
_____

Conformément à la loi suisse sur la protection des données (LPD), je dispose d'un droit d'accès et d'un droit de rectification.

J'ai en tout temps le droit de révoquer cette déclaration en tout ou en partie.

J'ai pris connaissance de l'annexe _____ .

Celle-ci décrit:

- des informations qui évaluent les risques d'atteinte à la personnalité (par ex. disponibilité, connectabilité);
- comment l'accès aux données est contrôlé;
- quels sont les pays dans lesquels les données peuvent être transmises et quelles sont les personnes (catégories) qui y ont accès;
- de quelle manière je peux retirer entièrement ou en partie mon consentement.

Lieu et date: Signature:

_____ _____

Par l'employeur
De plus en plus d'entreprises commencent à mettre à disposition des données relatives à leurs employés dans un annuaire électronique interne à l'entreprise et/ou accessible à des tiers pour consultation. C'est ainsi qu'il est possible en règle générale d'accéder au nom, à l'adresse ainsi qu'à d'autres paramètres de communication de collaborateurs ainsi que partiellement à des informations plus détaillées telles que qualifications, photographies, etc. De par le fait qu'elles apparaissent dans l'annuaire électronique d'un employeur donné, ces informations sont - même si elles sont accessibles au public comme dans le cas du nom et de l'adresse - sorties du contexte neutre d'un annuaire public pour être mises dans un contexte spécifique permettant par exemple de voir auprès de quelle société une personne donnée est employée. La connexion de données personnelles en soi anodines avec un tel contexte peut rendre ces données sensibles, par exemple dans le cas où un employeur est connu pour n'embaucher que des personnes appartenant à une religion précise ou partageant des idées politiques, idéologiques ou syndicales spécifiques.

En ce qui concerne le contrat de travail régi par le droit privé, l'article 328b du CO prévoit que l'employeur ne peut traiter des données relatives à l'employé que dans la mesure où celles-ci concernent son aptitude pour le poste de travail en question ou dans la mesure où elles sont nécessaires pour l'exécution du contrat de travail (voir p. 138 ss du présent rapport, ainsi que la p. 134 de notre 1er rapport d'activités). Cette disposition régit également la communication par l'employeur de données personnelles telles que le nom, l'adresse et autres paramètres de communication. Les données ne peuvent donc être communiquées que si cela est nécessaire pour l'exécution du contrat de travail. Ceci est le cas par exemple lorsqu'un employé a une fonction d'interlocuteur avec le public.
De même, il peut être nécessaire de communiquer les paramètres de communication d'un employé à un partenaire avec lequel on est en négociation, si l'employé en question fait fonction d'interlocuteur lors des pourparlers préliminaires ou des négociations contractuelles. L'article 328b CO ne prévoit cependant pas de registre général de tous les collaborateurs, accessible au public, à moins qu'une telle communication soit nécessaire pour l'exécution du contrat de travail.
Vu que l'article 328b CO (unilatéralement) est impératif, il n'autorise en aucun cas d'y déroger au détriment du travailleur, que ce soit par convention, contrat-type ou convention collective de travail. Une dérogation à l'article 328b CO en faveur de l'employé est par contre autorisée. La question de savoir si la communication de paramètres de communication d'un employé est en faveur ou en défaveur de la personne concernée dépend de la situation précise; une réponse ne peut donc pas être donnée à priori. Il est pensable qu'une communication générale des paramètres de communication puisse, selon le domaine d'activité de l'employeur (messageries roses, institutions religieuses ou racistes, sectes, etc.), avoir des conséquences préjudiciables pour l'employé. Des préjudices - bien que moindres - sont également envisageables dans d'autres cas. Une dérogation à l'article 328b CO n'est donc pas permise, même avec l'accord de l'employé.

Dans les cas où les conditions de l'article 328b CO ne sont pas remplies, la meilleure solution consiste à ce que l'employeur informe ses collaborateurs quant aux conséquences techniques et réelles (telles que consultation possible dans le monde entier, duplication des données) puis leur mette à disposition la plate-forme de l'annuaire électronique leur permettant de saisir eux-mêmes leurs propres

paramètres de communication, leur laissant ainsi la liberté de choisir le contenu et l'étendue des données communiquées, respectivement de les modifier et de les supprimer. En règle générale, les exigences relatives au caractère facultatif de la communication de données sont très élevées. Ceci vaut d'autant plus dans les rapports employeur/employé. Selon le climat de travail, suite à une pression exercée par d'autres ou à d'autres disparités de pouvoir - n'étant peut-être pas ressenties de manière consciente - le caractère facultatif apparent peut en réalité être le résultat d'une forte pression et de ce fait ne pas vraiment exister.

3.4. Extrait détaillé de la facture des PTT

Tout abonné au téléphone peut demander un extrait détaillé de la facture le concernant, avec indication de la date et la durée de la conversation, le montant de la taxe ainsi que le numéro appelé, tronqué des 4 derniers chiffres. Nous avons à plusieurs reprises reçu des plaintes de la part de personnes privées qui désiraient obtenir un relevé avec le numéro complet de l'abonné appelé.

Conformément à la Loi sur les télécommunications (LTC), les PTT sont en droit de communiquer à l'abonné les indications relatives à la date, à la durée et au montant des communications qui ont été effectuées sur ce raccordement. D'autre part, ils peuvent indiquer à quel central les numéros appelés sont raccordés. Le numéro complet de l'abonné appelé, ainsi que ses nom et adresse ne peuvent par contre plus être communiqués. La raison de cette restriction est en rapport avec la protection de tierces personnes qui sont amenées à faire des appels depuis l'appareil téléphonique de l'abonné. L'entreprise des PTT est soumise au secret des télécommunications. Elle n'est pas autorisée à communiquer à l'abonné quelles tierces personnes ont fait des appels depuis son raccordement avec qui et pour quelle durée, à moins qu'elle n'y soit obligée de par la loi. Cette réglementation peut cependant aboutir à des situations choquantes, par exemple dans les cas où le raccordement est utilisé exclusivement par l'abonné lui-même. La version actuelle a été décidée par le Parlement, conscient du fait qu'elle constituait un compromis entre l'intérêt de l'abonné d'obtenir un relevé de taxe complet et celui de tierces personnes utilisant le même raccordement et de leurs interlocuteurs à préserver la confidentialité de leurs conversations.

En 1993, une pétition adressée au Conseil National et demandant une modification des bases légales afin que les PTT puissent à nouveau établir un relevé de taxe complet, a été rejetée par la majorité de la commission du Conseil National. Une meilleure solution pour les abonnés qui utilisent seul leur raccordement peut tout au plus être trouvée dans le cadre d'une éventuelle révision de la LTC. Les projets de révision correspondants seront surtout empreints des questions de savoir si et comment prouver l'utilisation exclusive du raccordement par l'abonné, et si et comment les PTT seront en mesure de vérifier les indications faites. Aussi longtemps qu'il ne sera pas possible de trouver une solution permettant de distinguer clairement entre une utilisation du raccordement par des tiers (pouvant également être des invités) et une utilisation exclusive par l'abonné, et de permettre ainsi la vérification de l'utilisation exclusive du raccordement par le seul abonné, nous sommes d'avis que l'intérêt de l'abonné à obtenir un relevé de taxe complet doit céder devant l'intérêt des tiers à protéger leur personnalité.

3.5. Banque de données marketing de l'entreprise des PTT

L'entreprise des PTT est tenue d'opérer selon des principes reconnus de gestion d'entreprise. Comme toute entreprise gérée selon de tels principes, l'entreprise des PTT a intérêt à vendre ses produits et ses prestations de services à ses clients en fonction de leurs besoins. C'est la raison pour laquelle elle exploite une banque de données marketing pour sa clientèle commerciale dans le domaine de la poste et du trafic des paiements.

Cette banque de données marketing permet à l'entreprise des PTT d'offrir ses produits et ses prestations de services dans le domaine postal et du trafic des paiements en fonction des besoins du client. L'entreprise des PTT est tenue - comme tout autre organe fédéral - selon l'article 20, 2e alinéa, de l'OLPD de nous communiquer immédiatement, c.-à-d. déjà dès le début des travaux de développement, tout projet de traitement automatisé de données personnelles. Malgré cela, nous avons, en ce qui concerne le projet de la banque de données marketing, malheureusement été informés bien trop tard, alors que la décision de mettre sur pied cette banque de données avait déjà été prise.

Nous avons néanmoins pris position au sujet de ce projet et fait valoir les points de vue suivants:

- le traitement de données personnelles par les PTT dans cette banque de données marketing nécessite une base légale. Il n'existe pas de base légale explicite prévoyant une banque de données marketing, l'obligation légale d'exercer son activité selon des principes de gestion d'entreprise mise à part. Or, cette obligation constitue en principe une base légale suffisante pour exploiter une banque de données marketing, étant donné qu'une orientation vers le marché fait partie de la bonne gestion d'une entreprise. Cette orientation présume l'élaboration de concepts et de stratégies de marketing ainsi que leur mise en oeuvre. Afin de pouvoir offrir ses produits et ses prestations de services à ses clients existants de manière optimale et afin de pouvoir prendre soin d'eux, les entreprises ont besoin d'informations détaillées, utilisables à des fins de marketing, concernant les clients existants ainsi que les prestations auxquelles ces derniers sont abonnés. Les informations qui doivent être enregistrées dans la banque de données marketing sont des indications relatives à la clientèle commerciale qui sera prise en charge d'une manière orientée client.
- N'est cependant pas couverte par une base légale la communication de données personnelles à des tierces personnes, indépendamment du fait qu'il s'agisse d'un cas isolé ou d'une communication par procédure d'appel (online). Sont considérées comme tierces personnes non seulement les personnes physiques et morales extérieures à l'entreprise des PTT, tels que les partenaires commerciaux, mais également les unités internes et les employés des PTT qui n'ont pas absolument besoin des données personnelles en question pour l'accomplissement de leurs tâches. La communication à des tiers est par conséquent inadmissible, sauf si les données sont rendues anonymes.
- Des données personnelles ne peuvent être utilisées que dans le but indiqué lors de la collecte, qui découle des circonstances ou qui est prévu par la loi. L'utilisation de données relatives à des clients à des fins de marketing est en

principe, et selon l'article 2.1 *de la Recommandation no R (85) 20 du Comité des ministres aux États membres relative à la protection des données à caractère personnel utilisées à des fins de marketing direct,* couvert par le but original du traitement. Les informations relatives à la clientèle commerciale contenues dans la banque de données poste/trafic des paiements ne peuvent cependant être utilisées que dans le but d'assurer une prise en charge optimale des clients, donc par conséquent une gestion de l'entreprise conforme aux principes de gestion. Une utilisation à d'autres fins est inadmissible.

- Finalement, le traitement doit respecter le principe de la proportionnalité. Cela signifie que seules les données qui sont absolument nécessaires pour atteindre le but visé pourront être traitées. Plus spécifiquement, les champs libres (mémos) au sein de la banque de données marketing permettant de saisir des annotations en texte clair ne sont admissibles que si l'on ne peut absolument pas s'en passer. Ces champs ne peuvent contenir que les informations dont le conseiller de vente a absolument besoin pour accomplir sa tâche, à savoir conseiller le client. D'autres informations relatives à la clientèle commerciale telles que des indications qui n'ont aucun rapport avec les prestations postales pour les abonnés ou les prestations souscrites dans le domaine du trafic des paiements ne peuvent pas être traitées dans cette banque de données. D'autre part, seuls les conseillers de vente sont autorisés à introduire des informations dans ces champs libres. De même, l'accès à ces champs est réservé aux seules personnes qui y ont introduit des textes.
- En règle générale, l'accès aux données personnelles enregistrées à des fins de marketing est réservé exclusivement aux personnes et aux organes qui ont réellement besoin de ces données pour l'accomplissement de leur tâche. Cela signifie qu'un conseiller de vente ne doit avoir accès qu'aux données personnelles qui concernent les clients qui lui sont attribués. Pour l'élaboration de concepts et de stratégies de marketing, on peut travailler avec des données ayant été anonymisées, la connaissance de données personnelles spécifiques n'étant pas nécessaire. Même les personnes qui prennent des décisions au sujet des concepts de marketing n'ont pas besoin de consulter, voire de modifier les données de clients précis. Dans ce cas également, seul l'accès à des données anonymisées peut être justifié.
- L'exactitude des données et le droit d'accès doivent être garantis.
- Conformément à l'article 4.1.i. de la recommandation no (85) 20 mentionnée ci-dessus, toute personne concernée a le droit d'interdire que ses données soient utilisées à des fins de marketing. Cette exigence doit également être prise en considération dans le cas précis. Cela présuppose que les clients soient informés par les PTT de l'exploitation de cette banque de données marketing et que la possibilité leur soit donnée d'interdire l'utilisation des données personnelles les concernant.
- Finalement, le fichier doit être annoncé auprès du Préposé fédéral à la protection des données.

3.6. Perturbations au sein du réseau téléphonique de l'administration fédérale

Une grande partie des raccordements téléphoniques de l'administration fédérale à Berne sont reliés à un central téléphonique électromécanique vieux de plus de 20 ans. En raison de l'âge avancé de ce central et de l'immense charge à laquelle il est

soumis, des dérangements se produisent de plus en plus fréquemment, ce qui suscite des inquiétudes, surtout en ce qui concerne la protection des données.

Au printemps 1994, un collaborateur de l'administration fédérale a attiré notre attention sur le fait que des perturbations se produisaient dans le trafic téléphonique. Il nous a été rapporté que des tierces personnes pouvaient s'introduire dans une conversation téléphonique et l'écouter sans que les deux interlocuteurs s'en aperçoivent. Les dérangements concernent aussi bien des conversations internes à l'administration fédérale que des conversations établies entre des raccordements de l'administration fédérale et le réseau téléphonique public. Le service téléphonique de l'administration fédérale nous a confirmé que ces dérangements se produisaient, tout en relevant qu'ils étaient relativement rares par rapport à l'énorme volume du trafic.
Jusqu'au remplacement du central par un nouveau système numérique en novembre 1995, les unités administratives reliées à l'ancien central doivent faire preuve d'une vigilance accrue. Le service téléphonique s'efforce de limiter les dérangements en prenant des mesures de maintenance préventive. Les utilisateurs du téléphone ont par ailleurs été dûment informés par le service de sécurité de l'administration fédérale qui les a instruits de s'abstenir pour l'instant de communiquer des données confidentielles par téléphone. Vu que les utilisateurs ont été informés des risques et que le central sera remplacé d'ici fin 1995, la situation actuelle peut être tolérée d'un point de vue de la protection des données.

3.7. Responsabilité pour le transport de données par lignes électroniques

Lorsque des données personnelles sont transmises par courrier électronique (E-mail) ou mises à disposition pour consultation (annuaires électroniques), la question se pose de savoir qui est responsable de veiller au respect de la protection des données.

Les personnes privées et les organes fédéraux qui traitent des données personnelles sont tenus de garantir, par des mesures techniques et organisationnelles, la confidentialité, la disponibilité et l'exactitude des données. Si une personne privée délègue le traitement des données à une tierce personne, elle est tenue de veiller à ce que la tierce personne n'opère pas de traitement auquel elle ne serait pas autorisée elle-même (article 14 LPD). Un organe fédéral ne peut demander à un tiers de traiter des données personnelles que si ce dernier est en mesure de garantir la protection des données. Il reste cependant responsable de la protection des données et doit veiller à ce que les données soient traitées dans le cadre du mandat obtenu, surtout en ce qui concerne leur utilisation et leur communication. Si la tierce personne n'est pas soumise à la LPD, l'organe responsable devra s'assurer que d'autres dispositions légales offrent une protection des données comparable. Si tel n'est pas le cas, il devra garantir celle-ci par contrat.
Lorsque des données personnelles sont transmises par lignes électroniques ou mises à disposition pour consultation, les personnes mettant à disposition le réseau de communication sont également co-responsables de la confidentialité, de la disponibilité et de l'exactitude des données personnelles. La responsabilité principale incombe cependant aux personnes ou organes qui transmettent les données ou qui les mettent à disposition pour consultation. Ils sont en particulier responsables de garantir la protection des données sur les lignes de transmission et sur le réseau.

Toute personne mettant à disposition un réseau de communication doit cependant également veiller, dans la mesure de ses possibilités, à ce que la confidentialité, la disponibilité et l'exactitude des données soient garanties sur le réseau mis à disposition.

3.8. Télévision interactive

La télévision traditionnelle est un moyen de communication à sens unique. Tous les spectateurs regardent simultanément les émissions diffusées. Depuis un certain temps déjà, la discussion a été engagée à propos de la télévision interactive. Celle-ci permet au téléspectateur d'envoyer à son tour des signaux vers l'émetteur des programmes télévisés et ainsi d'exercer une influence sur le programme. Ce procédé génère cependant des données personnelles.

Jusqu'ici la télévision était par principe un moyen de communication à sens unique. Le spectateur d'une émission télévisée était un consommateur passif réduit à regarder ce qu'on lui proposait. Depuis un certain temps déjà, on parle de ce que l'on appelle la télévision interactive. Celle-ci permet au téléspectateur de quitter son rôle passif pour devenir un participant actif au programme télévisé. Sa participation est engagée depuis son fauteuil, dans son salon. Il existe plusieurs possibilités: participer à des émissions en direct, prendre influence sur l'action d'un film, participer à des jeux télévisés, effectuer des achats par le biais de l'écran de télévision (teleshopping) etc. Le système "Video on Demand" permet au spectateur de choisir un film parmi une série qui lui est proposée. Le film choisi sera alors diffusé spécialement et à titre individuel pour ce spectateur. Ce système permet à ce dernier de se concocter son propre programme. La réalisation de la télévision interactive nécessite une technique de transmission très coûteuse et n'est rendue possible que grâce aux effets conjugués des techniques de télévision et d'informatique.

La télévision interactive présente des risques considérables en matière de protection des données:

- lors de l'utilisation de la télévision interactive, l'enregistrement et l'analyse du comportement des spectateurs peuvent générer des données personnelles. Le traitement de données personnelles peut résulter de l'utilisation de l'offre elle-même ou servir à facturer les prestations dues. On peut ainsi enregistrer des informations sur les heures de présence, c.-à-d. que l'on enregistre qui profite à quel moment des possibilités de la télévision interactive. Ces indications sur le comportement (pendant les loisirs) d'une personne permet de voir si une personne regarde la télévision pendant la journée ou surtout le soir ou la nuit. Ceci permet en outre de tirer des conclusions sur les heures de travail, les habitudes de la personne (heures de sommeil, etc.).
- On enregistre ensuite des données relatives aux émissions visionnées, ceci à des fins de facturation. En enregistrant ces données, on dégage des préférences personnelles concernant les émissions, par exemple une préférence pour des émissions sportives, pour des films ou même pour certaines disciplines sportives, pour des émissions culturelles, des films érotiques ou des émissions politiques. C'est ainsi que peuvent être créés des profils de la personnalité.

- La fréquence des commandes ainsi que leur coût (par exemple pour le système "Video on Demand") permet de tirer des conclusions sur la situation financière d'une personne.
- Les données enregistrées en rapport avec les achats faits à distance (au moyen du système Téléshopping) permettent de tirer des conclusions sur la situation financière d'une personne et les produits qu'elle préfère.

  Les projets dans le domaine de la télévision interactive deviennent de plus en plus concrets. Les Télécom PTT ont prévu les premiers tests en Suisse pour 1995 (à Granges et à Nyon). Comme dans d'autre cas, l'entreprise des PTT a encore une fois manqué à son obligation légale de nous informer de ces projets dans leur phase initiale de développement. C'est la raison pour laquelle il ne nous est pas possible de vérifier leur conformité aux dispositions de protection des données. La seule constatation d'ordre général que nous puissions faire actuellement est que seules les données nécessaires pour l'exploitation technique de l'offre et pour une facturation correcte peuvent être enregistrées et conservées. Ces données ne peuvent être traitées que par les instances compétentes et ne devront en aucun cas être communiquées à des tiers sans l'accord du client.

3.9. Téléphoner sans argent comptant

Non seulement en raison du vandalisme croissant, mais aussi dans un souci d'épargner à leurs clients la nécessité d'avoir sur eux de la monnaie pour téléphoner, les compagnies téléphoniques remplacent de plus en plus les actuels appareils de téléphone publics par des systèmes fonctionnant sans argent comptant. Il existe plusieurs systèmes distincts, devant être appréciés de façon différenciée sous l'angle de la protection des données.

Les gens téléphonent de plus en plus sans argent comptant à l'aide de cartes en plastique. Il existe plusieurs types de cartes:

- d'une part, il est possible de téléphoner à l'aide de *cartes à prépaiement*. Dans ce cas, les conversations téléphoniques sont payées d'avance, comme lors de téléphones avec de l'argent comptant. En Suisse, cette carte appelée "taxcard" est en vente dans les bureaux de poste. Cette carte équivaut en valeur à un montant fixe que le client paie lorsqu'il achète la carte au bureau de poste. A chaque appel qu'il effectue depuis une cabine téléphonique publique, le montant équivalent à la conversation menée est débité de la carte. Cette carte n'est pas personnelle et peut être transmise à d'autres personnes. Le trafic de paiement effectué lors de l'utilisation d'une telle carte a lieu, comme lorsque vous téléphonez avec de la monnaie, dans l'anonymat complet. Cette manière de téléphoner ne pose donc aucun problème du point de vue de la protection des données. Il existe cependant aussi des cartes à prépaiement qui peuvent être rechargées auprès de stations de recharge. S'il s'agit de cartes anonymes, qui peuvent être rechargées moyennant paiement comptant par leur propriétaire sans code d'identification personnel (PIN), ceci ne pose également pas de problèmes du point de vue de la protection des données. D'autres pays utilisent cependant des cartes à prépaiement portant des signes distinctifs identifiant le propriétaire de la carte (par exemple un code PIN). Ces cartes peuvent être rechargées moyennant paiement

comptant ou au débit du compte de chèques postal. Le trafic de paiement effectué lors d'une conversation téléphonique reste bien anonyme, mais les opérations de recharge de la carte peuvent être attribuées au propriétaire de la carte.

- Un système bien différent des cartes à prépaiement est celui qui consiste à ne pas payer par avance, mais à débiter le montant de la conversation téléphonique une fois celle-ci terminée. Avec ce système, la personne qui effectue l'appel est identifiée à chaque appel. De plus, on enregistre à chaque appel des indications sur l'heure, la date et la durée de la conversation téléphonique ainsi que le numéro qui a été appelé. Le débit se fait dans ces cas sur un compte personnel du propriétaire de la carte. En Suisse, les PTT offrent depuis le mois d'avril 1995 la possibilité de téléphoner avec la *Postcard*. Ce système est basé - en tout cas dans un premier temps - sur la carte à puce "Postcard" existante et bien répandue des PTT. Les détenteurs de comptes de chèques postaux qui possèdent une Postcard peuvent donc utiliser leur carte non seulement au Postomat, dans les centres commerciaux, auprès des stations-services etc., mais aussi dans les cabines téléphoniques équipées à cet effet. La Postcard est introduite dans le lecteur avant l'appel, il suffit ensuite de taper le code personnel (PIN) pour pouvoir téléphoner. Les frais d'appels sont directement débités sur le compte de chèques du client. A partir des données enregistrées pour la facturation des appels effectués se développent ce qu'on appelle des profils de déplacement. Ces profils indiquent qui s'est trouvé quand à quel endroit. Il est en outre possible d'identifier les interlocuteurs sur la base du numéro appelé. C'est ainsi qu'on pose une trace de données qui n'est plus vérifiable par le client et qui est inquiétante du point de vue de la protection des données.
- En janvier 1995, les Télécom PTT ont lancé sous le nom de "Swiss Telecom Card" ce qu'on appelle une *Calling Card*. Avec ce système, utilisé surtout par les compagnies téléphoniques des États-Unis, le client appelle un numéro gratuit, spécifique au pays dans lequel il se trouve, pour être connecté au système de la compagnie qui lui a vendu la carte. Après avoir introduit son code personnel, il peut téléphoner autant qu'il veut. Qu'il téléphone depuis une cabine téléphonique publique ou depuis un raccordement privé ne joue pas de rôle dans ce cas. La facturation des conversations téléphoniques se fait en général au débit d'une carte de crédit. Ce système enregistre l'heure, la date et la durée des conversations ainsi que les numéros appelés et l'endroit à partir duquel les appels ont été effectués. Ces données sont communiquées au client sur la facture qu'on lui remet. Les numéros appelés apparaissent en partie directement sur le décompte de l'entreprise de cartes de crédit. Selon les demandes de souscription envoyées à leurs clients, les PTT proposent à l'abonné le choix entre un débit direct sur le compte de chèques postal, une facture mensuelle avec bulletin de versement ou un ordre de débit bancaire pour le débit automatique des factures des PTT. Le propriétaire de la carte peut en outre souscrire des cartes supplémentaires utilisables par d'autres personnes telles que des membres de sa famille ou des collaborateurs de son entreprise. Pour les conversations effectuées à l'aide de ces cartes supplémentaires, on communique sur la facture les indications suivantes: date et heure, durée et montant des conversations effectuées à l'aide des cartes supplémentaires, numéros appelés à l'aide de ces cartes et numéros des raccordements téléphoniques depuis lesquels les appels ont été effectués.

Les PTT ne nous ont pas informés des traitements de données prévus, ni pour le projet "Téléphoner avec la Postcard" ni pour le système "Swiss Telecom Card". Les PTT n'ont donc pas respecté leurs obligations conformément à l'article 20, 2e alinéa, de l'OLPD. Ces projets sont déjà réalisés ou le seront bientôt sans que des constatations détaillées puissent être faites sur la conformité des projets avec les exigences de la protection des données. Le fait qu'une utilisation abusive des "traces de données" générées par de tels systèmes peut provoquer des atteintes graves à la personnalité de certaines personnes semble sans aucun doute établi. C'est pourquoi la mise en oeuvre de mesures de sécurité appropriées s'impose. En ce qui concerne la Swiss Telecom Card, il reste également à vérifier si les données communiquées au propriétaire de la carte relatives au trafic effectué par les utilisateurs des cartes supplémentaires ne le sont pas en violation du secret des télécommunications tel qu'il est prévu dans la Loi sur les télécommunications ou des dispositions de cette dernière relatives à la facturation détaillée.

Le problème soulevé ici ne se limite pas au domaine des conversations téléphoniques. Les mêmes questions de protection des données se posent lors de l'utilisation d'autres systèmes de paiement tels que les achats sans argent liquide, l'achat sans argent comptant de titres de transport, etc.

3.10. Ordonnance relative aux données téléphoniques de l'EPFZ

L'école polytechnique fédérale de Zurich (EPFZ) désirait installer un système permettant un meilleur contrôle et une meilleure ventilation des coûts occasionnés par les appels téléphoniques. Elle nous contacta en nous priant de bien vouloir formuler les conditions à remplir, sous l'angle de la protection des données, pour l'exploitation d'un tel système de contrôle.

L'enregistrement de données en rapport avec une communication téléphonique réellement établie constitue un traitement de données personnelles. Ceci vaut aussi bien pour l'enregistrement de données appelées annexes (poste depuis lequel la conversation a été menée, numéro appelé, date, durée et montant de l'appel) que pour le contenu de l'appel proprement dit. En tant qu'organe fédéral, l'EPFZ n'est autorisée à traiter des données personnelles que dans les cas où une base légale suffisante existe. La collecte de données sensibles ou de profils de la personnalité doit en outre être reconnaissable pour la personne concernée. Dans le cas présent, nous sommes arrivés à la conclusion qu'une ordonnance administrative, qui régit les détails relatifs à l'enregistrement interne de données téléphoniques et à leur utilisation interne, constitue une base légale suffisante.

Cette base légale doit régir:

- quelles données de quelles conversations sont enregistrées,
- le but de l'enregistrement,
- dans quelles conditions certaines données relatives aux coûts par raccordement pourraient être communiquées à intervalles réguliers devant être fixés,
- quelles données sont contenues dans un relevé détaillé,

- quelles sont les conditions pour communiquer un relevé détaillé,
- la communication de relevés détaillés aux responsables des unités de gestion de l'EPFZ,
- la durée de conservation ainsi que les délais de destruction des données enregistrées.

La base légale doit également stipuler que les données téléphoniques peuvent être enregistrées exclusivement à des fins de contrôle des coûts. Une utilisation à d'autres fins, par exemple pour surveiller le temps de travail ou l'activité des collaborateurs ne serait donc pas admissible. Nous avons d'autre part retenu que seules peuvent être traitées les données qui sont absolument requises et nécessaires pour atteindre le but fixé. Cela signifie que les données enregistrées doivent être réduites au strict minimum nécessaire pour permettre un contrôle efficace des coûts. Il est donc admissible que soient enregistrés le raccordement d'où part l'appel, la date et la durée de la conversation, les taxes de conversation qui en résultent ainsi que le numéro appelé. Le numéro appelé devrait cependant être indiqué au moins sans les quatre derniers chiffres afin de rendre impossible une identification de la personne appelée, ceci n'étant pas nécessaire pour effectuer un contrôle des coûts. Il serait souhaitable que seul l'indicatif soit mentionné, dans la mesure où cela paraît suffisant. Seraient explicitement exclus du contrôle des coûts l'enregistrement des appels entrants et des conversations internes, celles-ci n'occasionnant pas de frais à l'EPFZ, de même que l'enregistrement du contenu des conversations.

Si des doutes ou des irrégularités apparaissent dans les enregistrements, il devrait être possible, tout en respectant certaines contraintes, de transmettre des relevés détaillés aux chefs des unités de gestion de l'EPFZ. Pour des raisons de transparence, une information aussi poussée que possible des collaborateurs concernant les données enregistrées doit avoir lieu. Celle-ci pourrait consister à remettre à chaque collaborateur le règlement administratif en vigueur, soit de manière directe (par ex. en le joignant au décompte de salaire) ou alors par voie de circulaire.

L'EPFZ a entièrement tenu compte de nos exigences dans le règlement administratif qu'elle a édicté. Nous pouvons dans ce cas présenter un exemple très positif de collaboration à un stade précoce.

4. Statistique

Recensement 2000

L'Office fédéral de la statistique (OFS) a entamé les préparatifs du recensement de la population de l'an 2000 et désire rationaliser à cet égard les méthodes de relevé afin de ne pas charger inutilement la population et les communes. Le recensement de la population se fera donc en partie sur la base des registres communaux du contrôle de l'habitant. Nous avons été priés de contrôler les mesures de protection des données du recensement, notamment l'utilisation ultérieure de celles-ci en vue de compléter les registres communaux.

Ainsi que nous en avons déjà fait état dans notre premier rapport d'activités (p. 122), l'OFS prépare d'ores et déjà le prochain recensement qui aura lieu en l'an 2000. Il

s'agit d'un projet de grande envergure et l'OFS entend à ce propos rationaliser les méthodes de relevé, organiser de manière plus efficace la collaboration entre les autorités cantonales et fédérales, permettre une utilisation optimale des données à diverses fins statistiques et limiter autant que faire se peut les inconvénients causés à la population.

Le recensement sur la base des registres cantonaux est l'outil principal capable à la fois d'améliorer la collaboration entre autorités et de rationaliser les méthodes de relevé, selon les cas aussi de réduire les inconvénients causés à la population. A l'article 4 de la nouvelle loi sur la statistique fédérale, le législateur a établi les principes régissant la collecte de données pour les relevés statistiques. Conformément à cette disposition, la Confédération renonce aux relevés lorsqu'un organe qui applique le droit fédéral dispose déjà des données requises. Le second alinéa du même article souligne expressément la possibilité du relevé indirect auprès des cantons ou des communes. Une condition est cependant posée: la statistique fédérale doit avoir besoin de ces données. Cette réglementation de la collecte de données pourrait être également appliquée au recensement s'il n'en résulte pas d'inconvénients pour la population.

Lors du recensement de la population de 1990, il a été exclu pour la première fois de réutiliser ultérieurement les données du recensement à des fins se rapportant à des personnes. L'introduction de l'article 3a de la loi fédérale sur le recensement fédéral de la population (loi sur le recensement) a codifié l'utilisation des données du recensement en conformité avec les principes de protection des données. Elle a en outre permis d'améliorer les rapports de confiance entre les citoyens et l'Etat. En vertu de ce nouvel article, un alinéa sur la garantie de la protection des données a été intégré à l'ordonnance sur le recensement fédéral de la population de 1990. Sept articles en tout veillent à un traitement conforme à la loi des données du recensement. Cette révision a tenu compte de la protection de la personnalité et constitue un grand pas en direction d'une protection plus efficace des données durant le recensement. L'OFS également a jugé de manière positive son expérience en relation avec la loi sur le recensement dans sa teneur de 1990, surtout du point de vue du droit de la protection des données.

L'option choisie par l'OFS, à savoir procéder à un relevé indirect des données essentiellement pour décharger la population (c'est-à-dire rassembler une partie des données directement à partir des registres des communes et des cantons et non pas en questionnant directement la population) est à juger de manière tout à fait positive. Néanmoins, même le relevé indirect de données (recensement à partir de registres) doit demeurer transparent pour les personnes recensées et celles-ci doivent pouvoir vérifier l'exactitude et la pertinence des données traitées et éventuellement les rectifier. Les données nécesssaires au recensement ne doivent en aucun cas être traitées à l'insu des personnes concernées. Il convient donc de prévoir tout d'abord la saisie des données contenues dans les registres, puis de faire remplir les parties manquantes du questionnaire par les personnes concernées elles-mêmes. Cette solution a l'avantage de permettre aux citoyens de contrôler les données relevées indirectement. On ne peut attendre de la population une collaboration fondée sur la confiance que si elle sait ce qu'il advient de ses données personnelles. L'expérience a montré qu'une coopération optimale entre population et autorités est indispensable au succès d'un recensement.

Il convient par ailleurs de veiller au respect du principe de finalité figurant à l'article 3a de la loi sur le recensement. Un recensement à partir de registres qui ne renonce pas au questionnaire direct ne doit pas servir à compléter les recueils de l'administration cantonale. Certes on peut comprendre qu'en vue de rationaliser leurs tâches, les communes aient besoin de compléter leurs registres par des données personnelles provenant du recensement. Néanmoins, cette utilisation ultérieure des données va à l'encontre du principe qui fonde la loi sur le recensement et exclut sans équivoque toute utilisation des données à des fins se rapportant à des personnes. Si l'administration utilisait les données à des fins autres que statistiques, elle se désolidariserait de la conception imposant une démarcation nette entre statistique et activité administrative et impliquerait un assouplissement, voire une modification des dispositions sur la protection des données introduites pour le recensement de 1990, ce qui nécessiterait en outre une modification de la loi sur le recensement. L'utilisation exclusive des données du recensement à des fins statistiques constitue par conséquent un élément essentiel de la confiance régnant à ce propos parmi la population. En effet, celle-ci donne des renseignements personnels en pensant avoir l'assurance que faite à des fins statistiques, cette communication n'impliquera pas d'inconvénients pour elle, en d'autres termes que ces données ne seront pas utilisées à des fins administratives. Ce genre d'inconvénients peut survenir car la somme des données personnelles relevées lors d'un recensement permet aisément la mise au point de profils complets de la personnalité, que l'on ne pourrait établir sur la base des recueils officiels du contrôle de l'habitant.

Il ressort clairement de la procédure de consultation qui a précédé la modification de 1990 de la loi sur le recensement que les données personnelles relevées à l'occasion du recensement doivent être traitées exclusivement à des fins statistiques. La réutilisation de ces données, en d'autres termes le contrôle et le complément éventuel des registres communaux à partir des données du recensement, a été rejetée.

Une modification de la pratique actuelle sur l'utilisation de ces données irait à l'encontre de la finalité fondamentale de la loi sur le recensement. En outre, elle se heurterait à la résistance de la population qui demande une séparation nette entre statistique et administration. Par ailleurs, le rapport de confiance encore chancelant entre les citoyens et l'Etat serait à nouveau ébranlé. C'est pourquoi la conception utilitariste des données du recensement ne devrait pas imprégner celle de l'utilisation statistique de ces mêmes données.

Le recensement fédéral de la population à partir de registres

Le recensement fédéral de la population de l'an 2000 se fera *en partie* par le relevé direct auprès de la population, *en partie* par le biais des registres. Pour pouvoir exploiter encore davantage les données des registres ou même procéder à un relevé uniquement indirect des données, il est essentiel d'harmoniser les registres communaux. C'est en effet le seul moyen de les utiliser de manière optimale pour le recensement. La tenue des registres relève de la compétence des cantons. Il faudrait donc au préalable modifier la constitution pour mettre en place une compétence fédérale réglementant cette harmonisation (cf. à ce propos notre 1er rapport d'activités, p. 122). Une modification aussi fondamentale des bases constitutionnelles paraît exclue pour le recensement de la population de l'an 2000; elle serait envisageable au plus tôt pour le recensement fédéral de l'an 2010.

5. Personnel

5.1. Secteur privé - rapports de travail

Les questions concernant les rapports de travail comptent encore parmi les préoccupations majeures émanant du secteur privé. Nous avons déjà présenté dans notre 1er rapport d'activités (p. 134 ss) nos principales observations à propos de la protection des données dans les rapports de travail au sein du secteur privé. Ces observations ainsi que d'autres qui sont venues s'y ajouter sont désormais rassemblées dans un guide qui s'adresse aux employeurs comme aux travailleurs. On peut le commander auprès de nos services. Nous donnons ci-dessous de brèves informations sur les dispositions en la matière et sur le contenu du guide, abordant un peu plus en détail la question de l'utilisation de systèmes de surveillance et de contrôle des travailleurs à leur poste de travail, thème d'une actualité croissante.

Situation juridique
Conformément à l'*article 328, 1er alinéa CO*, l'employeur est tenu de protéger et de respecter dans les rapports de travail la personnalité du travailleur. Il découle de cette disposition un devoir général d'assistance de la part l'employeur envers les travailleurs, devoir qui constitue la contrepartie du devoir de fidélité de ces derniers (article 321a CO). L'employeur doit s'abstenir de toute atteinte à la personnalité des travailleurs qui ne soit pas légitimée par le contrat de travail et parer dans le cadre des rapports de travail aux atteintes analogues des supérieurs, collaborateurs ou tiers. Le devoir d'assistance (également décrit comme obligation de s'abstenir de tout ce qui pourrait porter préjudice aux intérêts légitimes des travailleurs) implique également des limitations quant au traitement par l'employeur de données concernant les travailleurs. Ne serait-ce qu'en vertu de l'article 328 CO, les circonstances, qualités et dispositions personnelles qui ne contribuent pas essentiellement aux capacités professionnelles doivent demeurer inaccessibles à l'employeur. L'article 328 CO implique non seulement un devoir d'abstention, mais aussi une obligation d'informer les travailleurs de leurs droits, par exemple en les instruisant des conditions et de l'étendue des prestations sociales de l'entreprise, ainsi que des services sociaux disponibles. Il doit également informer les travailleurs des droits qui leur reviennent en vertu du droit de la protection des données, notamment du droit d'accès aux dossiers les concernant.

L'*article 328b CO* est entré en vigueur en même temps que la loi sur la protection des données. Il est ainsi libellé : "L'employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. En outre, les dispositions de la loi fédérale du 19 juin 1992 sur la protection des données sont applicables". L'article 328b CO prime la LPD et les autres dispositions générales de protection des données, mais est complété par les dispositions de la loi sur la protection des données. Il concrétise les principes généraux de traitement des données figurant à l'article 4 LPD, notamment celui de la proportionnalité. L'employeur est donc autorisé à traiter des données relatives aux travailleurs dans deux cas seulement et uniquement dans une mesure déterminée:

- dans le cadre de la conclusion d'un contrat de travail, il est autorisé à traiter des données concernant les candidats afin de déterminer leur aptitude à remplir l'emploi en question,

- durant les rapports de travail, il peut traiter les données nécessaires à l'exécution du contrat de travail.

Il ne peut être en aucun cas dérogé à l'article 328b CO, même avec le consentement des travailleurs (art. 362 CO).

La nouvelle *ordonnance 3 relative à la loi sur le travail* contient une disposition importante concernant la surveillance des travailleurs à leur poste de travail, sur laquelle nous reviendrons en détail un peu plus loin.

Guide pour le traitement des données personnelles dans le secteur du travail
Nous avons publié au printemps 1995 un guide traitant des questions les plus importantes inhérentes au traitement des données personnelles par des particuliers dans le domaine du travail. Ce guide reprend et complète les considérations figurant dans notre 1er rapport d'activités (p. 134 ss). Après quelques considérations générales sur la protection des données et sur le droit applicable, le guide traite, dans l'ordre chronologique, des questions de protection des données qui peuvent se poser au cours des rapports de travail. Pour ce qui est de la procédure d'engagement, il aborde entre autres la question de l'admissibilité des annonces sous chiffre, des indications données et des tests d'engagement, du traitement des données relatives à la santé, ainsi que de la question de l'obligation de restituer ou de détruire les données en cas de rejet d'une candidature. Il indique ensuite les données qui peuvent être traitées durant les rapports de travail, dans quelle mesure la personne concernée dispose d'un droit d'accès et d'un droit de rectification, quand les fichiers doivent être déclarés, et sous quelles conditions on peut communiquer des données à des tiers. Enfin, le guide examine la durée permise de conservation des données personnelles et le droit d'accès après la fin des rapports de travail. A propos de toutes ces questions, il est tenu compte des dispositions particulières du droit de la protection des données sur le placement et la location de personnel. Un chapitre particulier traite de l'utilisation des systèmes de surveillance et de contrôle sur le lieu de travail. S'agissant d'un thème d'une grande actualité, ce chapitre figure ci-dessous presque intégralement. Le guide peut être commandé gratuitement auprès de notre Secrétariat.

Utilisation de systèmes de surveillance et de contrôle des travailleurs au poste de travail
Sont considérés comme systèmes de surveillance et de contrôle tous les dispositifs techniques qui permettent d'observer, séparément ou par groupes les activités ou le comportement des employés. Ne serait-ce que pour des raisons de protection de la santé, l'employeur n'a pas le droit d'utiliser de tels systèmes s'ils sont destinés à surveiller le comportement des travailleurs à leur poste de travail (art. 26 de l'ordonnance 3 relative à la loi sur le travail). L'utilisation de systèmes de surveillance et de contrôle est par contre autorisée pour des raisons de sécurité et pour calculer le rendement (p. ex. enregistrement du nombre de frappes par jour dans un système d'élaboration de textes). Néanmoins, l'employeur ne peut utiliser de tels systèmes qu'après en avoir préalablement informé les employés concernés.

Font partie des systèmes de surveillance et de contrôle:

- l*es centraux téléphoniques*. Même de petits centraux téléphoniques, dont le coût n'est pas très élevé, permettent aujourd'hui d'enregistrer et d'établir le

relevé des appels qui entrent et qui sortent, y compris les numéros des abonnés, ainsi que la durée et le prix de chaque communication. Souvent aussi, il est très aisé d'écouter les conversations téléphoniques à l'insu des personnes concernées. L'enregistrement de données téléphoniques ne saurait avoir pour but de contrôler le comportement des employés. Le relevé des numéros d'abonnés dont le raccordement a été appelé *pour des raisons professionnelles* est admissible dans la mesure où il est effectué non pas pour contrôler le comportement des employés, mais bien pour des motifs d'ordre professionnel (p. ex. en vue de facturer la communication au client), et pour autant que les employés en soient informés. Un relevé des numéros d'abonnés à des *raccordements privés* que les employés composent (ou dont ils reçoivent des appels) ne doit en aucun cas être établi lorsque les conversations téléphoniques privées ne sont pas interdites d'une manière générale. Les indicatifs locaux peuvent, le cas échéant, être enregistrés. L'interdiction de tenir des conversations privées doit être imposée par des moyens autres que la surveillance des communications téléphoniques, par exemple en imposant l'établissement des communications externes via une centrale ou en ne permettant qu'à certains raccordements d'établir des communications directes. Lorsque le *numéro d'appel* s'affiche *automatiquement*, il convient de veiller à ce que l'affichage puisse, au besoin, être déconnecté par les deux correspondants. La transmission d'un appel à un raccordement autre que celui qui a été sélectionné doit être signalée à temps, de façon à ce que l'auteur de l'appel puisse interrompre la liaison. Le contenu de conversations téléphoniques ne peut être enregistré qu'à des fins de contrôle de performances (par ex. vente par téléphone ou objectifs didactiques) ou pour des motifs de sécurité. Cette mesure de contrôle éminemment incisive n'est admissible que si la personne dont la conversation est enregistrée ou écoutée y consent, et pour autant qu'elle en soit chaque fois informée à temps et de manière claire (par ex. par le biais d'un signal optique ou acoustique). Le rappel pour contrôle des abonnés appelés est *inadmissible* dans tous les cas. De même, l'écoute de conversations entre employés (par ex. par le biais d'un interphone équipé à cet effet) *n'est en aucun cas autorisée*. Lorsqu'une telle interdiction est en vigueur, les employés doivent avoir la possibilité, en cas d'urgence ou durant les pauses, de téléphoner depuis un raccordement non surveillé.

- *Les systèmes de TED*. Les systèmes de traitement électronique des données sont eux aussi dotés de nombreuses possibilités de surveillance et de contrôle. Au moyen de moniteurs intégrés au matériel ou au logiciel, il est par exemple possible d'enregistrer: le moment auquel un ordinateur est utilisé, si des configurations sont modifiées, les programmes qui sont actionnés ou déconnectés, les activités exécutées au sein d'un programme déterminé (mutations d'enregistrements, nombre de frappes par minute dans un système de traitement de textes, etc.). Les messages transmis par courrier électronique peuvent généralement être ouverts et lus sans difficultés.

- *Les autres systèmes.* Il convient de relever que d'autres systèmes, qui n'ont pas pour objectif premier de surveiller le personnel, peuvent être utilisés à cette fin (par ex. lorsqu'ils sont équipés d'un code d'accès électronique et d'un compteur automatique). Tel est par exemple le cas des photocopieurs, des

fax, des systèmes d'enregistrement du temps, des systèmes de déroulement des travaux, des contrôles d'accès, des compteurs, etc.

En cas de recours à des systèmes de *surveillance pour raisons de sérurité*, il convient de veiller à ce que le dispositif choisi ménage autant que possible les employés. Si par exemple, dans un grand magasin, une surveillance contre le vol est assurée par le biais de caméras vidéo, il convient d'éviter dans toute la mesure du possible que leur champ n'englobe les employés. Cette règle vaut également pour les installations de guidage de la production. Lorsqu'une surveillance des personnes elles-mêmes est nécessaire pour raisons de sécurité (par ex. pour être en mesure d'intervenir lors de situations dangereuses), il convient d'examiner des solutions de rechange (par ex. réponse à un message transmis à espaces réguliers, faute de quoi l'alarme se déclenche).

En règle générale, le recours à de tels systèmes doit s'accompagner de toute précaution utile. Ce principe est précisé dans les directives* suivantes de l'Organisation internationale du travail (OIT):

- les employés ont droit au respect de leur sphère privée sur le lieu de travail.
- Les employés doivent savoir quelles sont les méthodes de surveillance utilisées et connaître l'usage que l'employeur fait des données ainsi recueillies.
- L'employeur doit recourir aussi rarement que possible à des moyens de surveillance ou d'exploration des fichiers, des communications sur réseau ou du courrier électronique. La surveillance électronique permanente est interdite.
- Les employés doivent être associés aux décisions concernant l'opportunité et la manière d'utiliser les moyens de surveillance ou d'exploration.
- Des données ne peuvent être recueillies et utilisées qu'à des fins clairement définies et en rapport avec le travail.
- Il ne peut être procédé à des surveillances ou à des explorations sans information préalable des employés que si des indices sérieux permettent de présumer la commission d'actes criminels ou d'autres formes d'abus.
- L'évaluation des prestations des employés ne peut se baser uniquement sur les résultats d'une surveillance.
- Les employés ont le droit de consulter, de contester et d'exiger la rectification des données recueillies à leur sujet par le biais de la surveillance électronique.
- Les enregistrements qui ne sont plus nécessaires au but dans lequel ils ont été réalisés doivent être détruits.
- Les données recueillies lors d'une surveillance et qui permettent une identification individuelle des employés ne peuvent être communiquées à des tiers, à moins qu'une obligation légale existe à cet égard.
- Les employés ou les futurs employés ne peuvent renoncer au droit à la protection de leur sphère privée.
- Tout supérieur qui viole ces principes est passible de mesures disciplinaires ou de licenciement.

*Source :" A model employment/privacy policy", in Workers' privacy, Part II : Monitoring and surveillance in the workplace, Conditions of work digest, International Labour Office, Geneva 1993, p. 75. Traduction: PFPD, 3003 Berne.

5.2. Administration fédérale - tests d'aptitude, tel Sigmund Potentiel

Les mutations dans le traitement des données du personnel de l'administration fédérale ne se concrétisent pas seulement, comme nous l'avions relevé dans notre 1er rapport d'activité (p. 139/140), par l'introduction de systèmes décentralisés de traitement électronique. De plus en plus d'offices utilisent ou envisagent d'introduire, tant à des fins de recrutement que d'évaluation, des tests informatisés d'aptitude. Sigmund potentiel constitue un de ces outils de gestion des ressources humaines. En raison des risques pour la protection de la personnalité que représente le recours à de tels produits, il est impératif que leur cadre d'utilisation soit le plus strict possible. Finalement, toute la politique de gestion du personnel en sera modifiée, ce qui requiert une réflexion de fond et une concertation menée par l'ensemble des responsables de la gestion du personnel de la Confédération.

Rappelons tout d'abord que l'on entend par "tests d'aptitude" notamment les expertises graphologiques, les tests psychologiques, les tests de personnalité, les questionnaires biologiques, et les systèmes d'évaluation tel Sigmund potentiel. Pour que le recours à ce type de tests soit conforme à la loi fédérale sur la protection des données (LPD), ainsi qu'à la circulaire de l'Office fédéral du personnel concernant la protection des données (circulaire no 318.4/83 C. 2648), nous avons émis l'avis selon lequel les exigences suivantes doivent être remplies:

- l'information préalable du Préposé fédéral à la protection des données, ainsi que du conseiller à la protection des données de l'office ou du département concernés, s'il s'agit de produits tels Sigmund, pour examen sous l'angle de la protection des données;
- la création d'une base légale;
- le respect de principes généraux tels ceux de la finalité et de la proportionnalité;
- la fiabilité et l'objectivité des résultats;
- le caractère facultatif de la participation aux tests;
- le professionnalisme de la conduite des tests et de leur analyse;
- la compréhensibilité pour le candidat;
- l'anonymisation des tests dont les résultats sont envoyés à des experts externes ou au concepteur du test pour évaluation, respectivement amélioration de la qualité du produit;
- le contenu des questions respectueux de la personnalité des candidats;
- l'accessibilité des réponses et des résultats des tests uniquement au candidat et à l'évaluateur;
- la conservation séparée de ces informations, qui ne doivent pas être versées au dossier de la personne concernée;
- la destruction de ces données dans les meilleurs délais, à savoir dès que l'évaluateur a rédigé le rapport succinct nécessaire au futur employeur, mais au plus tard à la fin de la procédure de recrutement, respectivement d'évaluation. Le souhait de la personne concernée de conserver ces informations pour les comparer aux résultats d'un test ultérieur éventuel est réservé;
- la déclaration auprès de nos services du fichier constitué par les résultats des tests d'aptitude, si ceux-ci sont conservés au-delà du temps nécessaire à l'établissement d'un rapport d'évaluation.

En ce qui concerne le produit Sigmund potentiel, d'origine française, soulignons tout d'abord qu'il n'est pas destiné à se substituer à l'évaluateur, mais à structurer et orienter un entretien d'évaluation. Il s'agit non seulement d'un instrument de recrutement et de sélection interne et externe du personnel, mais encore et surtout d'un outil destiné à identifier des potentiels, orienter des carrières, détecter des besoins en formation etc.

Ce logiciel est mis à disposition sur un micro-ordinateur (PC). Il comprend 460 questions, toutes corrélées simultanément à plusieurs critères de personnalité qui sont au nombre de 38. 17 critères concernent la dimension professionnelle, 13 la dimension sociale et 8 la dimension psychologique. L'intéressé dispose de 9 secondes par question. Le questionnaire est en outre adapté aux caractéristiques régionales et culturelles du territoire sur lequel il est utilisé.

L'évaluateur n'a pas connaissance dans le détail des réponses données par la personne concernée, les résultats étant imprimés sous forme graphique, respectivement de notes attribuées à chaque critère de personnalité (entre zéro et vingt). Le taux d'adhésion au test est également donné. S'il est insuffisant, le test n'est pas utilisable par l'évaluateur.

Nous avons salué l'importance attachée par la responsable de Sigmund en Suisse au respect d'une éthique d'utilisation de son produit. En effet, elle n'octroie des concessions d'utilisation de logiciels de Sigmund qu'aux clients qui s'engagent contractuellement à respecter certaines règles, notamment de confidentialité. Elle recommande d'autre part la signature d'une charte d'utilisation de Sigmund, par laquelle l'évaluateur s'engage notamment à faire preuve de professionnalisme et à accepter le refus d'un candidat de passer le test.

Nous avons également souligné, sous l'angle de la protection des données, en particulier les avantages suivants:

- le test est sans cesse remis à jour;
- l'évaluateur n'a pas connaissance dans le détail des réponses données par la personne concernée;
- le test n'est utilisable que si le taux d'adhésion est suffisant;
- les résultats ne sont pas disponibles sous forme de texte prêtant à interprétation, mais sous forme de schémas;
- les résultats ne sont utiles que s'ils sont débattus avec le candidat au cours d'un entretien;
- les utilisateurs sont formés à l'emploi de Sigmund;
- un suivi de ces personnes est assuré par la responsable de Sigmund en Suisse afin d'éviter des "dérapages";
- la personne évaluée est dûment informée préalablement au test, et elle a droit à un feedback, ainsi qu'à l'accès aux résultats graphiques;
- les résultats du test ne sont accessibles qu'au candidat et à l'évaluateur.

Nous avons en revanche constaté les faiblesses suivantes:

- les résultats varient selon le moment où l'on procède au test, dépendant notamment de l'état du candidat, selon s'il vit ou non des problèmes personnels, professionnels ou familiaux;

- l'interprétation des résultats dépend avant tout de la personnalité de l'évaluateur, ainsi que de son expérience, de son sens de la psychologie, de sa sensibilité;
- un évaluateur expérimenté peut, s'il ne limite pas son entretien aux seules informations nécessaires à l'évaluation du candidat pour un poste déterminé, mettre à nu la personnalité de ce dernier, et s'il n'est pas doté du tact nécessaire, déstabiliser, voire perturber l'intéressé, et porter de la sorte atteinte à sa personnalité;
- le recours à Sigmund peut permettre de légitimer le rejet de candidatures non désirées en l'habillant d'objectivité;
- les notes fournies par Sigmund peuvent avoir des incidences négatives pour la personne concernée, si l'évaluateur est une personne "conventionnelle";
- la formation fournie par Sigmund n'est pas suffisante et ne garantit pas le professionnalisme requis.

Sur la base de ces constatations, nous avons requis, pour le recours à Sigmund à des fins de recrutement, non seulement le respect des principes susmentionnés relatifs aux tests d'aptitude, mais également que les conditions suivantes soient remplies:

- respect du principe de proportionnalité, qui implique en particulier que l'unité administrative a besoin, pour accomplir ses tâches légales, d'engager des agents présentant des qualités personnelles spécifiques difficiles à déceler sur la base d'un dossier ou des entretiens d'engagement habituels (esprit d'équipe, d'initiative, talents de négociateur ou de manager, autorité naturelle, forte résistance à l'échec...), ou doit repourvoir des postes de direction, voire des emplois particulièrement exposés;
- garantie d'un certain niveau d'objectivité par le recours à des experts extérieurs ou la mise en place d'un centre d'évaluation, par exemple à l'Office fédéral du personnel. Lors de chaque utilisation de Sigmund, l'expert, respectivement un agent de ce centre, assistent l'utilisateur ("Vieraugenprinzip"). Si un tel centre est instauré, il doit être dûment encadré et formé par la firme représentant Sigmund en Suisse;
- abandon des feuilles de notes;
- consultation du personnel avant l'introduction de Sigmund, comme le prévoit la circulaire de l'Office fédéral du personnel concernant la protection des données.

Quant à l'emploi de Sigmund à des fins d'évaluation de potentiel, nous avons souligné qu'il est à encourager et à promouvoir par les responsables de la gestion des ressources humaines des unités administratives utilisatrices de ce produit. Nous avons cependant signalé que de tels tests ne sont admissibles, outre les conditions susmentionnées, que s'ils sont effectués à la demande des personnes concernées.

L'utilisation de tests d'aptitude tel Sigmund au sein de l'administration fédérale comporte des risques sérieux d'atteinte à la personnalité. Il est donc impératif que le cadre d'utilisation de ces tests soit le plus strict possible. Ceci implique notamment l'adoption de directives détaillées par les départements concernés, lesdites directives intégrant aussi bien des exigences éthiques que de protection des données. Dans un deuxième temps, ces directives devront être intégrées dans la future ordonnance du Conseil fédéral concernant la protection des données dans le domaine du personnel, ordonnance déjà évoquée dans notre premier rapport (p. 148 ss). La

question de l'introduction d'une base légale au sens formel est quant à elle encore ouverte. Finalement, le recours à ces outils d'évaluation ne peut être bénéfique à l'administration fédérale et à ses agents que si la politique de gestion des ressources humaines est fondamentalement modifiée. Ceci implique une réflexion de fond conduite de concert par les représentants des responsables du personnel de la Confédération. La ligne commune ainsi dégagée garantira non seulement un standard législatif minimum en matière de protection des données, mais également un niveau d'éthique satisfaisant.

6. Assurances

6.1. Assurances sociales

En été 1994, nous avons été appelés à nous prononcer sur le statut des institutions de prévoyance de droit privé par rapport à la LPD, en particulier en rapport avec le devoir d'annonce de fichiers. Suite à notre intervention relative à la liste des analyses et tarif, évoquée dans notre 1er rapport (p. 138), un groupe de travail a été constitué. Il a notamment émis des propositions d'amélioration de ladite liste, entrées en vigueur le 15 mars 1995. Nous avons en outre été amenés à rappeler les principes régissant l'entraide administrative entre l'AVS et les autorités fiscales. Appelés à nous prononcer sur la légalité de la statistique du Concordat des caisses-maladie suisses (CCMS), nous avons finalement relevé que, sans être illégale, la situation de cette statistique n'est pas satisfaisante et requiert l'adoption d'un cadre législatif précis.

Droit de la protection des données applicable aux institutions de prévoyance de droit privé (ci-après les institutions) en matière de 2e pilier obligatoire, en particulier sous l'angle du devoir d'annonce de fichiers

Quel droit de la protection des données est applicable aux institutions? Qu'en est-il du devoir d'annonce? Ces questions, encore ouvertes à ce jour, ont été débattues notamment avec des représentants de l'Association suisse d'assurances (ASA). L'ASA a émis l'avis selon lequel les institutions sont soumises aux dispositions de la LPD applicables au secteur privé, opinion qu'elle a confirmée ultérieurement par écrit. Nous avons en revanche soutenu que les institutions sont assimilées à des organes fédéraux au sens de la LPD pour tous les traitements de données effectués dans le cadre du 2e pilier obligatoire, et ce pour les motifs suivants:

- les institutions accomplissent une tâche fédérale;
- le 2e pilier relève du domaine des assurances sociales, ce que le Conseil fédéral a confirmé dans son avis du 17 avril 1991 intitulé "Initiative parlementaire, droit des assurances sociales", concernant en particulier le projet de loi fédérale sur la partie générale du droit des assurances sociales;
- il ressort du commentaire de l'article 34quater de la constitution fédérale que c'est avant tout pour des raisons d'économie que le constituant a choisi de s'appuyer sur des structures existantes, anciennes pour la plupart et ayant déjà fait leurs preuves. Ce raisonnement avait déjà été tenu dans d'autres secteurs des assurances sociales telle l'assurance-maladie, sans que cela

préjuge du statut des caisses, considérées comme organes fédéraux par la LPD;
- l'affiliation à une institution est obligatoire;
- les contestations entre institutions de prévoyance, employeurs et ayants droit ne sont pas réglées selon la procédure civile, mais selon la procédure administrative. En effet, au niveau fédéral, la voie du recours de droit administratif au Tribunal fédéral des assurances est ouverte;
- si l'on se réfère à l'ordonnance du Conseil fédéral sur la création de la fondation fonds de garantie LPP, les subsides versés aux institutions de prévoyance sont assimilables à des subventions;
- dans le cadre des travaux relatifs à l'Espace économique européen, la Commission des Communautés européennes a émis l'avis selon lequel la prévoyance minimale obligatoire doit être considérée comme partie intégrante d'un système de sécurité sociale. Le Parlement, malgré la vive opposition des milieux concernés, a avalisé ce point de vue.

Ceci implique en particulier que les institutions de prévoyance privées doivent, pour ce qui relève du 2e pilier obligatoire, annoncer tous les fichiers concernés auprès de notre Secrétariat.

La liste des analyses et tarif (la liste)
Nous avions évoqué les problèmes de protection des données posés par la liste dans notre 1er rapport (p. 138). Nous étions alors dans l'attente d'une décision de constitution d'un groupe de travail chargé de réviser la liste, puis d'examiner dans sa globalité la problématique des flux d'informations à destination des caisses d'assurance.

Le groupe de travail ADAK a été constitué par décision du Département fédéral de l'intérieur du 25 avril 1994. Entre le 24 juin et le 15 novembre 1994, l'ADAK a tenu quatre séances au cours desquelles des propositions d'amélioration de la liste ont été faites (entrée en vigueur: le 15 mars 1995) et un inventaire global des problèmes de flux d'informations établi, assorti de propositions de solutions. Nous tenons ici à souligner le caractère particulièrement fructueux de la collaboration qui s'est instaurée au sein de ce groupe.

Nous avons cependant constaté, au cours de ces travaux, ainsi que lors de l'examen du projet d'ordonnance du Conseil fédéral sur l'assurance-maladie, que la liste en tant que telle, même améliorée, est problématique sous l'angle de la protection des données, à l'instar des autres listes utilisées en matière d'assurance-maladie. Nous avons toutefois émis l'avis que l'emploi de ces listes est admissible tant qu'elles n'auront pas été remplacées par d'autres systèmes de contrôle des coûts, actuellement à l'étude, à la fois plus efficaces et respectueux de la protection des données.

L'obligation des organes de l'AVS de renseigner les autorités fiscales (article 50, alinéa 1bis de la loi fédérale sur l'AVS)
Ce nouvel alinéa est entré en vigueur le 1er janvier 1995, simultanément à la loi fédérale sur l'impôt fédéral direct. Il supprime l'obligation de garder le secret des organes de l'AVS à l'endroit des autorités chargées de l'exécution des lois fiscales. Sur la base de cette disposition, la Conférence des fonctionnaires fiscaux d'Etat avait demandé à recevoir systématiquement certaines informations. Nous avons été

consultés à plusieurs reprises sur l'étendue de l'obligation d'entraide incombant aux organes de l'AVS. Nous sommes parvenus à la conclusion selon laquelle le caractère obligatoire mis à part, cette norme s'inscrit dans la ligne des principes généraux de l'entraide administrative, que l'on peut résumer en ces termes:

- une base légale prévoit expressément la communication d'informations;
- une demande motivée est déposée dans un cas d'espèce;
- les renseignements sont nécessaires à la législation fiscale;
- les informations n'ont pas pu être collectées auprès du contribuable ou de son employeur.

La statistique du Concordat des caisses-maladie suisses (CCMS)
Nous avons tout d'abord relevé que l'utilisation du terme "statistique" est impropre tant du point de vue de la législation sur la statistique que de celle sur la protection des données, du moment que la statistique du CCMS est tenue de manière nominative (par fournisseurs de prestations) et ne poursuit pas à titre principal un but statistique mais plutôt de contrôle de l'économie des traitements.

Consultés par une personne privée en juillet 1994 en particulier sur la question de la légalité de la statistique du CCMS, nous avons tout d'abord constaté que le Tribunal fédéral des assurances admet dans une jurisprudence constante le recours à cette méthode pour établir l'existence d'une polypragmasie (Ueberarztung). Il n'est cependant pas entré en matière sur la question de la légalité de la statistique du CCMS, semblant considérer que la disposition de la loi sur l'assurance-maladie consacrant le principe du caractère économique des traitements constitue une base légale suffisante. Après examen de cet article de loi, ainsi que du contenu de la statistique du CCMS à la lumière de la LPD, nous avons considéré que le principe de la légalité n'est pas violé, pour peu que cette statistique soit utilisée comme instrument de contrôle du caractère économique des traitements.

Nous avons cependant souligné que la situation actuelle n'est pas satisfaisante, cette statistique étant convoitée par un nombre toujours plus grand d'utilisateurs potentiels, d'où risque de violation du principe de finalité en l'absence de cadre juridique précis. D'autre part, les caisses-maladie et les autorités de surveillance sont, en tant qu'organes fédéraux, responsables du respect de la protection des données qu'ils traitent ou font traiter. Ces organes ne peuvent le faire que par voie contractuelle, ce qui n'est pas satisfaisant. En outre, avec l'entrée en vigueur de la nouvelle loi sur l'assurance-maladie prévue pour 1996, la question de "la co-habitation" de la statistique du CCMS avec d'autres statistiques, telles celles que gérera l'Office fédéral des assurances sociales se posera avec de plus en plus d'acuité. Finalement, la responsabilité de la statistique du CCMS incombe tant à des organes fédéraux qu'à des personnes privées, ce qui rend la situation quelque peu confuse. Nous avons donc conclu, pour des raisons de transparence et de sécurité du droit notamment, qu'il est nécessaire de doter dans les meilleurs délais la statistique du CCMS de bases légales spécifiques, à ancrer dans un premier temps dans une ordonnance d'exécution de la nouvelle loi sur l'assurance-maladie, puis dans la loi lorsque cette dernière fera l'objet d'une révision.

Il ressort des paragraphes qui précèdent que, s'il est vrai que les lacunes relevées par le rapport Jaggi voilà plus de dix ans sont encore loin d'être comblées, il n'en demeure pas moins que, dans le domaine des assurances sociales, la sensibilisation

à la protection des données va croissant, et que l'on prête plus d'attention à la LPD et à ses exigences.

6.2. Assurances privées - feuille d'information et clause de consentement

Les assurances privées sont en principe tenues de par la LPD de nous déclarer leurs fichiers, vu que le traitement de la plupart de ces données n'est pas soumis à une obligation légale et que les personnes concernées n'en ont pas suffisamment connaissance. La plupart des assureurs ont privilégié la solution de l'information à celle de l'annonce de leurs fichiers. Cette information s'est généralement faite par le biais d'une feuille d'information ("Merkblatt") et par une formulation plus détaillée de la clause de consentement ("Einwilligungsklausel"). Cette reformulation n'a pas seulement été effectuée pour faire preuve de transparence, mais également pour que ladite clause permette aux assureurs de lever le secret médical sans violer ce dernier. Ces documents ne nous ont pour la plupart pas été soumis avant leur diffusion, et nous y avons relevé un certain nombre de lacunes et d'imprécisions. Nous avons en particulier constaté que la formulation trop générale de cette clause équivaut à un blanc-seing pour les assurances, ce qui n'est pas conforme aux exigences de la protection des données. Finalement, nous avons émis l'avis selon lequel la solution retenue par certains assureurs, de ne prévoir qu'une seule clause standard de consentement, utilisable par tous les secteurs de l'assurance privée, est également contraire à la LPD. En effet, la masse et la fréquence des flux d'informations nécessaires à la gestion d'un dossier ne sont par exemple pas les mêmes dans l'assurance-vie que dans l'assurance-maladie complémentaire.

7. Santé

7.1. Distribution de drogue sous surveillance

Les essais de distribution de drogue sous surveillance ne sont pas non plus incontestés du point de vue du droit de la protection des données. Dans l'intérêt des participants, les essais devraient être effectués de manière anonyme. Et c'est d'ailleurs ce qui est prévu dans l'ordonnance en question. Pourtant, on rencontre de la résistance sur de nombreux fronts. Il a notamment été exigé que les participants déposent leur permis de conduire auprès du service des automobiles lors de l'essai.

La renonciation à toute transmission à des tiers des données concernant les participants au test a rencontré parfois une vive opposition, avant tout de la part des autorités administratives ou de police. Ainsi, les services des automobiles justifièrent leur opposition en alléguant que, comme la participation au projet impliquait la consommation de drogues et que cela excluait la possibilité de conduire un véhicule à moteur, le permis de conduire devait être déposé chez eux. Si, par contre, le permis est déposé volontairement auprès d'un responsable du projet, le fait de conduire un véhicule n'aurait alors comme pire conséquence qu'une amende sanctionnant le fait de ne pas avoir le permis de conduire avec soi; alors que dans l'autre cas cela provoquerait une procédure disciplinaire. Rappelons que le dépôt du permis de conduire auprès du service des automobiles a le même effet qu'un retrait. Une mesure aussi contraignante ne saurait être imposée délibérément aux

participants; d'ailleurs, elle n'est pas prévue dans *l'ordonnance du 21 octobre 1992 sur l'évaluation de projets visant à prévenir la toxicomanie et à améliorer les conditions de vie des toxicomanes,* ordonnance qui règle les détails de l'essai.

Seules les personnes ayant donné leur accord écrit peuvent participer à l'essai (déclaration de consentement, voir les particularités y relatives dans notre 1er rapport d'activités, p. 133-134). Ce consentement ne peut être demandé qu'après une information orale et écrite détaillée sur les conditions de l'essai. La personne concernée est informée qu'il est interdit de conduire un véhicule à moteur durant sa participation au projet et que la conduite d'un véhicule à moteur sous l'influence de stupéfiants est punissable. Elle s'engage à déposer son permis au début du projet auprès d'un responsable du projet. En outre elle donne son accord quant à l'évaluation scientifique du projet et se déclare également prête à participer, sous certaines conditions, telles qu'elles sont émises dans la déclaration de consentement, à des évaluations et analyses. A cela s'ajoute notamment le fait de rendre anonymes toutes les données nécessaires à l'évaluation scientifique. Des données relatives à la personne, collectées par des interviewers externes, ne sont pas transmises à des tiers, ni même au projet. De cette façon, il est impossible que les réponses aux questions posées puissent avoir des conséquences personnelles pour les personnes concernées. Afin d'obtenir des indications relatives à la criminalité liée au trafic de drogue, malgré le postulat d'anonymat, la direction du projet recueille un extrait du casier judiciaire lors de l'entrée de tout participant au projet, et un autre lors de sa sortie. Mais, dans cette démarche également, dans le but de maintenir la garantie d'anonymat des participants à l'essai, la participation à cette étude n'est pas mentionnée auprès du casier judiciaire central.

Comme la pratique l'a mis en évidence, la plupart des participants ne possèdent pas de permis de conduire. Cependant, la suppression de l'anonymat due au dépôt du permis de conduire auprès du service des automobiles pourrait entraîner une réduction sensible du taux de participation au projet. Cela aurait à son tour des incidences négatives sur l'évaluation scientifique des mesures de prévention et d'assistance et, finalement, sur le développement de nouvelles possibilités de traitement.
Lors de la pesée d'intérêts entre l'intérêt public lié à la sécurité routière et celui de procéder à l'évaluation scientifique des essais contrôlés de distribution de drogue sous surveillance, il faut tenir compte aussi bien du nombre modeste de participants (au début 1995, seules quelque 320 personnes, la plupart sans permis de conduire, participaient au projet) que de la durée limitée du projet, soit fin 1996.

Sur la base de ces réflexions, nous sommes arrivés à la conclusion que le dépôt du permis de conduire auprès des responsables de projet, pendant la durée de la participation, était préférable au dépôt auprès du service des automobiles, notamment en raison de l'atteinte à la personnalité qui peut découler de la suppression de l'anonymat.

7.2. Logiciels de démonstration

Pour les démonstrations de logiciels, l'on ne devrait utiliser des données personnelles qu'avec l'assentiment des personnes concernées. Sinon il faut

accorder la préférence à des noms de fantaisie afin d'être sûr de ne léser personne dans sa personnalité.

Nous avons été consultés par un développeur de logiciels qui voulait savoir si une version d'un paquet de logiciels contenant des données mélangées sur des patients, et utilisable à titre de démonstration pour ergothérapeutes et physiothérapeutes, respectait la protection des données. Les données de base qui devaient être traitées consistaient en nom, prénom, adresse, sexe, état civil, date de naissance, numéro de téléphone, profession et employeur, ainsi que la caisse maladie sans le numéro d'affiliation. Ces données personnelles, en relation avec les diagnostics médicaux et les traitements prescrits, doivent être considérées comme sensibles.
Il nous a tout d'abord paru étrange que, dans le cas d'espèce, l'accès à de véritables données de patients par un développeur de logiciels fût déjà tout simplement possible. Selon l'article 321 du code pénal, les médecins ainsi que leurs auxiliaires (p. ex. les physiothérapeutes) sont en effet soumis au secret professionnel lorsqu'on leur en confie un dans le cadre de l'exercice de leur profession. Une divulgation de cette information est punissable sur plainte. La personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalité portés à sa connaissance dans l'exercice de sa profession, laquelle requérant la connaissance de telles données, se rend punissable. Il en va de même des données personnelles portées à la connaissance des personnes soumises au secret professionnel dans le cadre de leur activité professionnelle (art. 35, 1er et 2e alinéas, LPD). Pour ces raisons, la transmission, par des physiothérapeutes, de données exactes relatives à des patients, sans l'assentiment de ces derniers, est interdite; par conséquent le traitement de ces données par le développeur de logiciels n'est pas admissible.
Il en irait autrement si ces données étaient mises volontairement à disposition par les personnes en cause; dans ce cas, rien ne s'opposerait à leur traitement. Toutefois ces personnes devraient être informées au préalable avec précision du but de l'exploitation des données, de la période durant laquelle elles seraient traitées, des modalités de transmission de ces données à des tiers et, enfin, de la destruction desdites données. Finalement, les personnes en question devraient donner leur accord exprès écrit. Si tel n'est pas le cas, il faut utiliser des noms de fantaisie ou des désignations numériques.
Si de véritables anamnèses ("Krankengeschichten") sont utilisées pour démonstration, elles ne peuvent être diffusées par le maître du fichier qu'après avoir été rendues anonymes. Or, une anamnèse n'est anonyme que lorsqu'une personne ne peut pas être identifiée, même sur la base d'une combinaison déterminée de données (par exemple la description d'une maladie rare).

7.3. Maintenance de logiciels

Des mesures spéciales doivent être prises pour la maintenance d'un système TED par des personnes externes. Il se peut que l'accès du fournisseur aux données personnelles qui figurent dans le logiciel soit indispensable. Toutefois le maître du fichier devrait ôter chaque fois que c'est possible les données personnelles de l'ordinateur avant les travaux de maintenance.

Le fait de confier des travaux de maintenance sur un ordinateur n'équivaut pas à donner accès aux données personnelles, mais offre tout de même la possibilité de

prendre connaissance des données saisies dans l'ordinateur. Si la maintenance permet l'accès à des données sensibles, une protection particulière est nécessaire. La protection doit être garantie par des mesures techniques et organisationnelles ("Vier-Augen-Prinzip"). Les dispositions pénales de la LPD doivent être respectées. Se rend punissable la personne qui, intentionnellement, aura révélé d'une manière illicite des données personnelles secrètes et sensibles ou des profils de la personnalités portés à sa connaissance dans le cadre des activités qu'elle exerce (article 35, 2e alinéa, LPD).
Le maître du fichier ferait bien de conclure avec le fournisseur un "Non-Disclosure-Agreement". Au mieux, une telle convention figure déjà dans le contenu du contrat de maintenance.

7.4. Droit d'accès du patient à son dossier - participation aux frais

Toute personne peut demander au maître d'un fichier de connaître les données traitées à son sujet. Ceci est également valable pour les données que le médecin traite à propos de ses patients. Nous avons dû examiner à quelles conditions le médecin peut demander du patient une participation aux frais pour la consultation de son dossier.

Après une thérapie de plus de dix ans, une patiente a demandé à son médecin une copie de son anamnèse, écrite à la main. Le médecin était d'accord sur le principe, mais voulait toutefois savoir à quelles fins ses notes manuscrites seraient utilisées, et soumit à la patiente un devis estimatif pour les copies, dans lequel il a également tenu compte du temps que cela prendrait. La patiente, de son côté, était d'avis que le droit d'accès pouvait être exercé gratuitement et contesta le devis.
En principe, toute personne peut demander au maître d'un fichier si des données la concernant sont traitées, et quelles sont ces données. Elle doit requérir cette information par écrit et justifier de son identité au maître du fichier. Les renseignements sont, en règle générale, fournis gratuitement et par écrit, sous forme d'imprimés ou de photocopies. Comme l'exercice du droit d'accès est l'émanation du droit fondamental de la liberté individuelle, il doit pouvoir en principe être revendiqué indépendamment de l'acquittement d'une taxe.
L'ordonnance relative à la loi fédérale sur la protection des données prévoit une exception au principe de la gratuité lorsque les renseignements désirés ont déjà été transmis à la personne concernée dans les douze mois précédant sa demande, et que l'on ne peut pas rendre vraisemblable un intérêt légitime à la fourniture de renseignements. On parle d'intérêt légitime notamment lorsque les données personnelles ont été modifiées à l'insu de la personne concernée. Mais une participation aux frais peut aussi être demandée lorsque la remise des informations est liée à un volume de travail particulièrement important. Cela peut être le cas par exemple, si le fichier a été géré manuellement et exclusivement dans des buts internes, et n'est pas équipé pour la communication des données. A l'avenir, les maîtres de fichier doivent faire en sorte que leurs fichiers soient organisés de manière à permettre aux personnes concernées l'exercice de leur droit d'accès et de rectification.
L'émolument s'élève à 300 francs au maximum. Le requérant doit être informé du montant de la participation avant la délivrance des renseignements et peut retirer sa requête dans un délai de dix jours. On peut exiger une "participation équitable", mais pas les coûts réels de l'opération.

Dans le cas présent, nous avons conseillé à la patiente de demander au médecin si elle pouvait venir consulter son dossier sur place. Cette manière de procéder permet d'une part de réduire les coûts et d'autre part d'éclaircir d'éventuels malentendus. En outre, cela peut éviter les problèmes de déchiffrement propres au manuscrit. Les renseignements pourraient, le cas échéant, aussi être donnés oralement pour autant que le requérant soit d'accord avec ce procédé. Au cas où les informations relatives à la santé de la personne concernée sont par trop délicates, il est conseillé de les confier à un médecin neutre en qui le patient a confiance, afin qu'il les lui communique.

7.5. Dons de sang - questionnaire médical

Celui qui veut faire don de son sang doit tout d'abord remplir un questionnaire médical de la Croix-Rouge Suisse afin que la fiabilité du don puisse être contrôlée. Ces conditions répondent à des impératifs de sécurité inhérents au don de sang. Toutefois le remplissage de ce questionnaire suscite parfois une certaine opposition due à des investigations qui, à certains égards, portent fortement atteinte à la sphère intime.

Une personne qui voulait donner du sang et qui aurait dû remplir un tel questionnaire, a été irritée par l'orientation de certaines questions. Il s'agissait entre autres de questions relatives aux relations sexuelles, à la consommation de drogues, aux vaccinations, aux piqûres de tiques, aux voyages dans les régions de malaria, aux grossesses et traitements hormonaux. Comme le questionnaire devait être complété par d'autres indications et archivé par la suite, la personne concernée refusa de répondre à toutes les questions; pour cette raison, elle ne put pas donner son sang. Elle s'est adressée à nous pour savoir si les questions et leur traitement ultérieur étaient admissibles.
Comme il ressort d'une notice remise aux personnes concernées avant qu'elles ne remplissent le questionnaire, la Croix-Rouge Suisse est consciente que ces questions vont loin dans la sphère privée des donneurs. Le questionnaire médical représente toutefois une mesure importante pour garantir au bénéficiaire la meilleure sécurité possible quant à la qualité du sang. Pour le moment la Croix-Rouge Suisse est soumise aux dispositions relatives au traitement des données personnelles par des personnes privées. Celui qui exploite des données personnelles en tant que personne privée n'a pas le droit de léser de manière illicite la personnalité des personnes en cause. Une violation de la personnalité peut être justifiée entre autres par le consentement du lésé. Dès le moment où le donneur fournit volontairement les indications exigées, il autorise l'examen de la qualité de son don. Ainsi le traitement des données nécessaires à l'exécution du don de sang est justifié.

8. Crédits

Liste de mise en garde en matière de crédits

A différentes reprises des associations mettent à la disposition de leurs membres des listes complètes sur la solvabilité de clients potentiels. Toutefois, la remise systématique et globale à des tiers de listes de mise en garde pose de graves

problèmes de protection des données. Nous nous sommes vus dans l'obligation d'émettre une recommandation au sujet du traitement de telles données.

Une association s'est adressée à nous pour savoir dans quelle mesure ses listes de mise en garde en matière de crédits étaient compatibles avec la LPD. Les membres de l'association signalaient à son secrétariat les clients qu'ils avaient poursuivis ou ceux qui étaient régulièrement en retard dans leurs paiements. Le secrétariat compilait les noms de ces clients et leur situation financière sur des listes de mise en garde en matière de crédits et remettait régulièrement ces dernières à tous les membres de l'association.
Comme nous l'avons mentionné à l'association, la remise systématique à ses membres de listes de mise en garde n'est pas conforme à la protection des données. Il est préférable de fournir de telles informations de cas en cas, et uniquement sur demande. Les fichiers concernés doivent en outre nous être annoncés, car les personnes concernées n'ont pas connaissance du traitement desdites données.
Sur ce, l'association a maintenu, qu'à son avis, les listes de mise en garde étaient, en tant que moyen de protection des créanciers, aussi admissibles d'après la LPD et qu'elles n'étaient pas soumises à une obligation d'annonce. En outre, on ne pouvait pas parler d'une communication de données personnelles à des tiers, simplement parce que cela apportait une indépendance économique aux membres de l'association. La communication de données personnelles au sein de l'association ne devait pas être considérée autrement qu'une communication de données internes à une entreprise. Un traitement cas par cas de demandes relatives à la solvabilité entraînerait d'énormes dépenses et des coûts supplémentaires déraisonnables, ce qui rendrait tout à fait illusoire la protection interne en matière de crédit. En outre, un règlement prévoyait que la liste ne pouvait être utilisée que pour l'examen de la solvabilité de clients potentiels.
Suite à cela, nous avons émis une recommandation selon laquelle l'association devait arrêter de suite l'expédition systématique et globale de listes de mise en garde contenant nom, adresse, indications sur la situation financière et éventuellement des données sur des poursuites et faillites de clients potentiels. Ce genre d'informations ne pouvait être données que sur demande et de cas en cas. Le fichier concerné devait en outre nous être annoncé.

En raison de cette recommandation, l'association a renoncé à la saisie systématique et à la communication de listes de mise en garde en matière de crédits et développé un concept TED "contrôle des débiteurs". Ce concept nous a été soumis et contient les réglementations suivantes:

- L'association établit un règlement dans lequel figurent les conditions-cadres de l'utilisation du système TED. En plus, un contrat est conclu avec chaque utilisateur du système qui l'oblige à ne contrôler que la solvabilité des clients avec lesquels des relations d'affaires existent ou sont envisagées, ou avec qui des contrats ont été ou seront conclus. Sur la base de la réglementation contractuelle, il n'est pas nécessaire d'exiger une preuve d'intérêt légitime pour chaque demande. Les membres ont l'obligation de ne fournir que des indications exactes et de ne pas transmettre à des tiers les renseignements obtenus. L'ancien système de la liste de mise en garde est aboli. Actuellement, les données sont introduites trimestriellement dans une banque

de données. A l'avenir, ces annonces auront lieu chaque mois. L'actualité et l'exactitude des données sont assurées par l'association.

- Techniquement, le système TED est organisé de telle sorte que seule la consultation cas par cas est possible. Le feuilletage des champs de données n'est pas admis. L'utilisateur ne peut employer comme critères de recherche que le nom, l'entreprise ou le numéro de la taxe à la valeur ajoutée (caractéristiques évidentes d'identification) du client.
- Les données communiquées sur papier à l'association sont conservées pendant une année puis détruites. Toutes les données enregistrées dans le système sont, durant la première année, effacées tous les trois mois et réécrites; ensuite, cette procédure aura lieu chaque mois. La provenance des informations sur la solvabilité peut être vérifiée à tout moment par l'association afin de respecter l'obligation de renseigner. Le fichier doit nous être annoncé.

9. Droit de bail

9.1. Formulaires d'inscription pour locataires

Nous avons émis une recommandation concernant les renseignements que le bailleur est en droit de demander lors du choix d'un ou d'une locataire.

En décembre 1993, nous avons reçu pour examen des formulaires d'inscription destinés aux personnes désireuses de louer un appartement. Nous avons donc entendu les associations concernées dans des hearings et élaboré une première appréciation, que nous avons soumise pour consultation à ces associations et à d'autres personnes concernées. Nous avons par ailleurs examiné un nombre considérable de formulaires d'inscription couramment utilisés (cf. à ce propos notre 1er rapport d'activités, p. 152 ss).

Notre enquête a donné les résultats suivants:

- le traitement de données personnelles en relation avec la location d'un logement est soumis à la LPD. Ce traitement ne constitue pas un traitement de données personnelles à des fins exclusivement personnelles, cas dans lequel la LPD ne serait pas applicable.
- Tout traitement de données en relation avec la location d'un logement ne se justifie pas par le fait que les éventuels futurs locataires en ont connaissance ou qu'ils ont eux-mêmes fourni les renseignements. Les traitements de données qui contreviennent aux principes généraux de traitement ou qui portent atteinte d'une autre manière à la personnalité des locataires éventuels ne sont justifiés que par le consentement que la personne concernée a donné en connaissance de l'atteinte.
- Le bailleur ne peut pas faire valoir dans tous les cas un intérêt prépondérant au traitement des données. Certes, il traite des données personnelles en relation avec la conclusion d'un contrat de bail, ce qui justifie en principe un traitement de données. Mais cela n'est valable que pour le traitement de données concernant l'autre partie au contrat et dans la mesure où la conclusion du contrat le requiert. Les traitements de données qui vont plus loin, par exemple des renseignements absolument inutiles au choix du locataire ou portant sur

des personnes qui n'entrent absolument pas en ligne de compte, sont de ce fait injustifiés. Plus les personnes sur lesquelles des données sont collectées avant la conclusion d'un contrat sont nombreuses, plus il s'impose de faire preuve de réserve lors de la collecte et du traitement de données sur ces personnes puisque le traitement de données concernant la plupart d'entre elles n'est pas en relation directe avec la conclusion du contrat de bail.

- Les obligations légales qui nécessitent une collecte de données relative aux futurs locataires (par exemple l'obligation d'annonce au contrôle de l'habitant) ne justifie pas que ces renseignements soient demandés à toutes les personnes intéressées au logement.
- La collecte de données ne doit pas être illicite (par ex. demander si la personne est disposée à signer un contrat d'assurance avec l'agence immobilière en question). Ladite collecte ne doit pas aller à l'encontre de la bonne foi (par ex. demander la marque de la voiture de la personne désirant louer le logement afin de pouvoir estimer sa capacité financière), ni être disproportionnée. Il ressort des formulaires examinés que le bailleur fonde en premier lieu son choix sur la situation financière de la personne en question et désire ensuite savoir si elle a un mode de vie susceptible de gêner les autres locataires. Les questions ne se rapportant pas à ces deux domaines sont considérées comme disportionnées et inadmissibles. En outre, les recherches nécessaires doivent se faire avec tous les ménagements possibles envers le futur locataire. Par exemple le bailleur n'a pas besoin de demander si cette personne est fiancée, mariée, séparée, divorcée ou veuve, afin de savoir si le logement servira de domicile familial au sens du droit matrimonial. Il lui suffit de demander si le logement servira de domicile familial.
- Enfin, les données ne doivent pas être utilisées à d'autres fins que le choix du locataire adéquat et la conclusion du contrat de bail. Elles ne seront pas transmises à des tiers et seront protégées par des mesures techniques et organisationnelles appropriées contre tout traitement non autorisé. Une fois terminée la procédure de choix, toutes les données à l'exception de celles concernant le locataire choisi doivent être immédiatement détruites.

Sur la base de ces réflexions, nous avons conclu qu'il convient de différencier quatre catégories de données :

- celles qu'il faut collecter dans tous les cas,
- celles qui ne doivent être collectées que s'il existe une obligation légale (par ex. obligation d'annonce des étrangers à la police des étrangers),
- celles qui ne doivent être relevées que dans des conditions particulières (par ex. disposition statutaire selon laquelle une coopérative de logements ne loue qu'à des personnes accomplissant une formation),
- enfin celles qu'il ne faut en aucun cas collecter (par ex. maladies chroniques).

Nous avons réparti en quatre catégories les questions figurant sur les formulaires que nous avons examinés et à partir de là, nous avons rédigé une recommandation s'adressant à tous les bailleurs du pays. Cette recommandation a été publiée dans la Feuille fédérale et fournie aux associations et personnes concernées entendues lors des hearings et de la procédure de consultation qui a suivi.

Plusieurs bailleurs ont rejeté la recommandation en totalité ou en partie. Dans telle situation, le préposé fédéral à la protection des données peut soumettre le cas à la

commission fédérale de protection des données pour décision, ce qui fut fait en février 1995. L'affaire est maintenant entre les mains de la commission.

9.2. Communication d'informations relatives aux bailleurs de logements pour invalides

L'Office des constructions fédérales nous a consulté pour savoir s'il était licite de remettre à l'Association suisse des invalides une liste de tous les logements pour invalides ayant bénéficié d'une aide fédérale. Les données communiquées comportent l'adresse du bien-fonds en question, le nom et l'adresse du maître d'oeuvre, la date du début de la location et le nombre de logements pour invalides.

La communication de données ne pose aucun problème lorsque les personnes concernées en sont informées et ont la possibilité de la refuser. Nous avons donc conseillé à l'Office des constructions fédérales de signaler à l'avenir - lors de l'octroi de subventions aux logements pour invalides - que des données seront éventuellement communiquées à une ou plusieurs associations d'invalides explicitement nommées, et de donner aux personnes concernées la possibilité de s'opposer à cette communication. Pour ce qui est des logements déjà construits, informer les personnes concernées demanderait une somme de travail énorme. Mais puisque les logements pour invalides subventionnés par la Confédération ne doivent être loués qu'à des invalides, il est permis de supposer que les bailleurs ont en principe intérêt à ce que les locataires potentiels qui remplissent les conditions aient connaissance de ce genre d'appartements. Par ailleurs, si seule l'adresse de l'immeuble en question était communiquée, les personnes intéressées se verraient obligées de requérir en divers endroits des renseignements sur la personne du bailleur. Ces démarches peuvent représenter pour les invalides un surcroît de difficultés considérables et ne signifie pas nécessairement davantage d'égards pour le bailleur.
Pour ces raisons et après avoir pesé les intérêts en jeu, nous avons approuvé la communication des logements construits sans information préalable des bailleurs. Nous avons assorti cette approbation des conditions suivantes pour limiter au maximum le risque de communication indésirable :

- chaque fois qu'une occasion se présente, donc même après la communication, il convient d'informer les personnes concernées.
- Seules les adresses utiles à la location des logements en question doivent être communiquées (donc, le cas échéant, celle de l'agence immobilière et non celle du maître d'oeuvre ou du propriétaire).
- Lorsqu'une personne concernée s'oppose à la communication de données, celles-ci ne doivent pas être transmises ou si la communication a déjà été effectuée, il convient de veiller à ce que les associations d'invalides ne transmettent pas plus loin l'adresse en question et qu'elles la rayent de leurs fichiers.
- Les associations d'invalides ne doivent communiquer les adresses qu'à des personnes entrant en ligne de compte en tant que locataires et uniquement à cette fin. Nous avons en outre conseillé de procéder à une répartition des logements par région pour éviter de remettre à chaque fois la liste complète des adresses.

On ne pourrait dispenser l'Office des constructions fédérales de la nécessité d'obtenir le consentement des personnes concernées que s'il était créé à cet effet une base légale dans l'ordonnance relative à la loi encourageant la construction et l'accession à la propriété de logements.

II. AUTRES THEMES

1. Vente par correspondance

Nous trouvons dans nos boîtes aux lettres les envois postaux les plus divers. Un grand nombre de ces envois relèvent de la publicité, souvent accompagnée d'une proposition d'achat. Ce phénomène quotidien, la plupart du temps anodin, peut avoir des répercussions parfois très désagréables.

On nous a signalé l'an dernier le cas suivant: un enseignant reçoit à l'adresse de son école un bon pour l'achat d'accessoires pornographiques. Hormis le fait qu'il n'a jamais commandé un objet de ce genre, il est fortement gêné de recevoir une telle offre sur son lieu de travail. En outre, il figure par erreur sur le bon en tant que "Madame". Toute cette affaire lui est très pénible. Il s'adresse donc à nous et nous consulte sur la manière de riposter à ce genre d'envoi.

Nous lui avons conseillé de faire valoir son droit d'accès afin de déterminer comment et pourquoi son adresse avait été utilisée à cette fin. La maison de vente par correspondance répondit qu'elle avait reçu à son nom une commande pour cet "appareil", mais qu'elle n'était pas en mesure d'en vérifier l'origine car les commandes étaient passées aussi bien par écrit que par téléphone. Elle se déclara prête à effacer les données personnelles de cet enseignant de son fichier-clients. Ce dernier voulut néanmoins savoir d'où la maison de vente par correspondance tenait son adresse afin de la faire rayer aussi du fichier d'où elle provenait. Il trouvait choquant que cette entreprise ne contrôle pas la provenance des commandes reçues, surtout d'objets aussi "délicats", et s'appuyait à ce propos sur l'article 5 LPD qui oblige le maître d'un fichier à s'assurer que les données personnelles qu'il traite sont correctes. Ce genre de contrôle s'impose surtout lorsqu'une commande n'est pas signée. Dans des cas comme celui-ci, il convient en outre de s'assurer que la commande n'émane pas de mineurs.

L'enseignant porta l'affaire devant les tribunaux en déposant une plainte pénale. Le tribunal constata que les dispositions pénales de la loi sur la protection des données n'avaient pas été enfreintes, mais admit que le traitement erroné des données personnelles du plaignant dû à la négligence pouvait se traduire par une atteinte à sa personnalité. Les frais de justice furent donc mis à la charge de la maison de vente par correspondance. Fort de ce jugement, l'enseignant voulut introduire une action en dommages-intérêts, à laquelle il renonça en définitive par crainte de frais trop élevés car le code de procédure civile de son canton de domicile prescrit une *représentation légale obligatoire*. Il est regrettable que l'exécution des droits d'une personne lésée soit empêchée par des règles de procédure. Il conviendrait peut-être de se demander si dans les cas d'atteinte à la personnalité, la procédure civile

pourrait être simplifiée comme pour les actions en exécution du droit d'accès selon l'article 15, 4e alinéa, LPD.

2. Radiation de l'annuaire des numéros 156 des PTT

L'entreprise des PTT tient un annuaire accessible au public qui recense toutes les personnes exploitant un numéro 156. Nous avons été confrontés au problème de l'identification possible des adresses privées de personnes offrant des services érotiques par le biais d'un numéro 156 dans le cas où le raccordement téléphonique se trouve à l'adresse privée de cette personne.

L'entreprise des PTT à accepté que les personnes qui offrent de tels services depuis leur adresse privée ont le droit envers les PTT de faire bloquer ces données afin de protéger leur personnalité. Si une telle personne exerce ce droit de blocage, elle ne sera pas recensée dans l'annuaire 156 ou, si elle y figure déjà, elle en sera rayée.

3. Envoi de factures / expédition sans enveloppe

Nous trouvons presque chaque jour dans nos boîtes aux lettres toutes sortes de factures de provenances diverses. Des factures de téléphone, d'électricité, de loyer et de médecin sont envoyées pour la plupart sans enveloppe et accessibles à chacun. Une facture peut, suivant le type de relation contractuelle, contenir diverses données personnelles.

La plupart des factures contiennent l'identité des partenaires contractuels ainsi que la somme due. Quelques unes en revanche révèlent le type de relation contractuelle et diverses caractéristiques du contrat qui permettent de déduire des particularités de la personne concernée inhérentes notamment à son comportement, ses conditions de vie, son appartenance sociale, sa situation financière et autres.

Une personne nous a fait part de son opposition au mode d'acheminement sans enveloppe de factures relatives aux primes d'une assurance. Cette dernière s'était refusée à adresser de telles factures sous pli fermé, étant d'avis que les montants facturés ne constituaient pas des données relevantes sous l'angle de la protection des données. Or, toutes les données concernant une personne tombent dans le champ d'application de la LPD, pour peu que ces informations se rapportent à une personne identifiée ou identifiable. Il n'existe de ce fait aucune "donnée libre". De plus, dans le cas des primes d'assurance, il ne s'agit pas que de montants à payer, mais également de factures contenant diverses sommes et données qui permettent notamment de tirer des conclusions quant au type de prestation d'assurance.

Lors de l'envoi de telles factures, les principes généraux de la LPD sont à observer, dont celui de la proportionnalité. Il est conforme à ce principe d'envoyer les factures concernant des primes d'assurances sous pli fermé. Le secret postal n'est opposable qu'au fonctionnaire des PTT et ne protège pas les factures expédiées sans enveloppe contre un accès par des tiers non autorisés. Or, l'article 7, 1er alinéa, LPD prévoit que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures techniques et organisationnelles appropriées. Selon l'article 8, 1er alinéa, de l'ordonnance du 14 juin 1993 relative à la LPD (OLPD), la

personne privée qui traite des données est tenue en particulier d'assurer leur confidentialité. Ceci implique notamment une protection des informations contre les modifications, copies, accès ou autre traitement non autorisés (lettre e). Ces exigences sont également valables pour les organes fédéraux (article 20, 1er alinéa, OLPD). Finalement, les mesures techniques et organisationnelles requises à l'article 8, 2e alinéa, OLPD, doivent être appropriées. Pour ces motifs, nous sommes d'avis que les factures ne peuvent pas être expédiées sans enveloppe, leur envoi sous pli fermé étant une mesure susceptible de garantir de manière appropriée la protection des données.
Plusieurs sociétés ont déjà adopté une telle pratique.

4. Données personnelles officielles figurant dans les registres privés

La consultation téléphonique automatisée de données est une pratique de plus en plus courante. On peut ainsi obtenir par Telekiosk ou Vidéotex les informations les plus diverses, de la recette de cuisine aux programmes de concert. Mais certains particuliers offrent aussi par ce biais des informations plus délicates. Nous avons donc élaboré une recommandation sur l'admissibilité des registres privés de personnes.

Nous nous sommes déjà exprimés dans notre 1er rapport d'activités (p.144) sur l'admissibilité des registres de la propriété concernant les véhicules en leasing, volés ou saisis. Nous en avions conclu que, pour peu que certaines conditions soient remplies, il n'y avait aucune objection à la tenue de ce genre de registres, notamment parce qu'ils ne contiennent que des données personnelles que la personne concernée a transmises en sachant qu'elles seraient réutilisées. Au cours de l'exercice écoulé, nous avons examiné s'il était admis d'exploiter un registre consultable automatiquement, contenant des renseignements sur des inhumations, tutelles et faillites privées publiés dans les feuilles officielles. Les données contenues dans le registre avaient été recueillies dans diverses feuilles officielles ou autres publications officielles et étaient accessibles à tous sans qu'il soit nécessaire de justifier d'intérêt. Le maître du fichier invoquait le fait qu'il s'agissait de données publiées, donc officielles, dont la réutilisation était admise sans autres considérations. Nous n'avons pu nous rallier à cette argumentation car :

- la constatation de l'état civil, dont les *décès*, est en principe du ressort de la Confédération. Pour des raisons de sécurité du droit et de protection de la personnalité, la tenue de banques de données privées, accessibles au public, contenant des renseignements relevant de l'état civil ne peut être admise en parallèle aux registres publics de l'état civil tenus à cet effet (mais non librement accessibles).
- Les particuliers possèdent un intérêt justifié à être informés du crédit des personnes avec lesquelles ils entrent en relations économiques, par conséquent de recevoir des informations sur d'éventuelles *ouvertures de faillites*. La loi fédérale sur la poursuite pour dettes et la faillite en tient compte dans la mesure où elle prévoit que quiconque justifie d'un intérêt peut avoir accès aux procès-verbaux tenus par les offices des poursuites et faillites et s'en faire remettre des extraits. De même l'ouverture et la clôture de la procédure de faillite doivent être communiquées publiquement. Il n'en ressort cependant pas que les données relatives aux faillites et aux saisies doivent être rendues

directement accessibles à tous. Une saisie centralisée, systématisée et automatique de toutes les faillites ouvertes, éventuellement avec communication automatique aux personnes concernées, recèle un risque beaucoup plus grand d'atteinte à la personnalité que les publications prévues par la loi ou la possibilité de prendre connaissance des procès-verbaux des offices des poursuites et faillites sur la base d'un intérêt justifié. Dans le cas que nous avons examiné ici, ce risque s'est justement vu confirmé par le fait que la personne demandant le renseignement ne doit pas justifier d'un intérêt, et qu'il n'est donc pas exclu qu'elle s'informe par pure curiosité ou dans un but précis d'atteinte au crédit.

- La *mise sous tutelle* d'une personne majeure doit être publiée dans la feuille officielle de son domicile ou de son lieu d'origine dès qu'elle entre en force. Une nouvelle publication de la tutelle est prévue si la personne en question change de domicile. Ces dispositions ont pour but de protéger les tiers de bonne foi, vu que les personnes mineures ou mises sous tutelle ne peuvent s'engager par leurs actes qu'avec le consentement de leur représentant légal. Si la tutelle est levée, les tiers de bonne foi n'ont plus besoin d'être protégés. Mais, dans le registre dont il est ici question, la tutelle demeure constatable après la fin de la mesure, ce qui constitue une grave atteinte à la personnalité de la personne concernée, atteinte qui ne trouve pas de motif justificatif dans d'éventuels intérêts de tiers. Par ailleurs, les sanctions administratives telle la mise sous tutelle font partie des données sensibles dont la communication à des tiers constitue une atteinte à la personnalité en vertu de l'article 12, 2e alinéa, lettre c LPD.

L'exemple figurant dans la documentation publicitaire de l'exploitant du registre, faisant état d'un chef du personnel pouvant apprendre par ce biais si un candidat avait été quelque temps auparavant condamné à une peine privative de liberté, montre précisément l'ampleur du risque d'abus et d'atteinte à la personnalité dû à la saisie et à la communication systématique de ce genre de données sur les tutelles. Conformément à l'article 328b CO, le (futur) employeur ne peut traiter des données concernant le travailleur que dans la mesure où ces données portent sur les aptitudes du travailleur à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail (cf. p. 138 ss). Déterminer si un candidat a été condamné à une peine d'emprisonnement n'est donc permis que si les données recherchées sont essentielles pour évaluer l'aptitude du candidat à remplir son emploi. Mais même dans ce cas, l'employeur ne peut recueillir les données sans l'assentiment du candidat et sans lui dire pourquoi il doit éventuellement demander un extrait de son casier judiciaire. Il est manifeste que la possibilité d'être informé d'une mise sous tutelle sans justifier d'un intérêt peut mener également dans d'autres cas à des atteintes à la personnalité.

Dans les trois domaines abordés, nous en sommes donc arrivés à la conclusion que la saisie centralisée et systématique de données dans des registres de personnes afin de les communiquer par consultation online ou sur demande à qui s'y intéresse n'est pas conforme à la protection des données, car de tels traitements de données sont en principe réservés aux interventions de l'Etat. Il convient donc de considérer ces fichiers comme illlicites et la communication de ces données comme un détournement de leur finalité.

Sur la base de ces considérations, nous avons recommandé à cet exploitant de fichier de s'abstenir à l'avenir du traitement de données concernant les décès, les faillites et les mises sous tutelle.

5. Recherches généalogiques

La pratique de la généalogie requiert la consultation de nombreux documents officiels auprès des autorités cantonales et fédérales les plus diverses. En de nombreux cas, aucun texte ne fixe si ce genre de consultation est autorisé et à quelles conditions. Depuis l'entrée en vigueur de la LPD, les généalogistes ont de plus en plus de difficultés à obtenir de la part des autorités la permission de consulter les registres. La situation juridique varie selon que l'on désire consulter des registres de l'état civil, des registres publics relatifs aux rapports juridiques de droit privé, ou encore d'autres documents officiels.

Recherches dans les registres de l'état civil et dans d'autres registres publics relatifs aux rapports juridiques de droit privé
La LPD n'est pas applicable aux registres publics relatifs aux rapports juridiques de droit privé (article 2, 2e alinéa, lettre d LPD), dont font également partie les registres de l'état civil. Ce sont surtout ces derniers que l'on consulte dans le cadre de recherches généalogiques. Ils relèvent de l'ordonnance sur l'état civil, laquelle prescrit que les particuliers n'ont pas accès aux registres de l'état civil. Exceptionnellement, les autorités cantonales de surveillance peuvent octroyer aux particuliers le droit de consulter les registres de l'état civil si elles considèrent comme fondée la demande de consultation. De nombreux cantons permettent en général la consultation des registres de l'état civil à des fins de recherche généalogique, souvent en l'assortissant de charges. Il est recommandé d'adresser par écrit une demande dûment motivée aux autorités de surveillance du canton dans lequel les recherches doivent être faites. Les parents en ligne directe ainsi que les personnes qui rendent vraisemblable un intérêt légitime peuvent demander un extrait des inscriptions au registre. Si la requête porte sur des renseignements concernant des personnes encore vivantes, les personnes concernées demanderont elles-mêmes un extrait du registre ou donneront dans ce but procuration à la personne qui fait les recherches. Pour le reste, il n'est en général accordé à des tiers aucun renseignement sur des personnes encore vivantes.

Malheureusement la situation juridique relative aux recherches généalogiques dans les registres de l'état civil est encore insatisfaisante; en effet, ce cas n'est pas réglé expressément dans l'ordonnance sur l'état civil et l'octroi des renseignements demandés ou leur refus sont laissés à l'appréciation des cantons. Néanmoins, il est prévu prochainement de réglementer expressément ce cas dans l'ordonnance sur l'état civil.

Recherches dans d'autres documents officiels
Dans ce cas, la LPD n'est applicable qu'aux données communiquées par des organes fédéraux alors que la communication de données personnelles par les autorités cantonales relève du droit cantonal de la protection des données. La situation juridique dans les cantons est diverse. Tous ne disposent pas d'une loi sur la protection des données et celles qui existent présentent parfois des différences considérables. Là aussi, il est conseillé de déposer par écrit auprès des autorités

dont on attend des informations une demande dûment motivée de consultation et de se faire expliquer par celles-ci la situation juridique.

L'octroi de renseignements par des *organes fédéraux* est soumis aux prescriptions suivantes :

- si la personne concernée est décédée, l'article 1er, 7e alinéa, OLPD prévoit que le renseignement doit être donné lorsque le requérant justifie un intérêt à la consultation et qu'aucun intérêt prépondérant de proches de la personne décédée ou de tiers ne s'y oppose. Un intérêt est établi entre autres en cas de proche parenté. Conformément à cette disposition, il convient donc en général (lorsqu'il n'est pas nécessaire de garder le secret par égard aux proches) de donner suite à une demande de consultation concernant des parents décédés à des fins de recherches généalogiques.
- Si la personne concernée n'est pas décédée, la communication des données est soumise à l'article 19 LPD (et éventuellement aux dispositions du le droit des archives). Conformément à cette disposition, les organes fédéraux ne sont en droit de communiquer des données personnelles que s'il existe une base juridique. Or la communication de données concernant des personnes vivantes à des fins généalogiques n'étant prévue nulle part, elle n'est donc pas autorisée. Même s'il n'existe pas de base légale, les organes fédéraux peuvent exceptionnellement communiquer sur demande le nom, le prénom, l'adresse et la date de naissance d'une personne dans la mesure où cette communication ne contrevient pas aux principes généraux de la protection des données. Les recherches généalogiques peuvent justifier une telle exception; chaque cas doit néanmoins être apprécié selon les circonstances. Là également, il convient d'adresser une demande aux autorités compétentes.

6. Les 350 personnes les plus riches et les plus influentes de Suisse

La publication "Les 350 personnes les plus riches et les plus influentes de Suisse" est une compilation de données personnelles qui est communiquée à des tiers. Si cela s'effectue sans que les personnes concernées le sachent, le fichier doit alors nous être annoncé.

Cette publication regroupe des indications sur le nom, l'adresse, la profession/activité, la propriété, la branche et la fortune de 350 personnes. En outre, elle contient encore une brève biographie de la plupart des personnes d'une à deux pages, contenant des informations supplémentaires portant sur la formation, les activités professionnelles et autres, les relations, les contacts avec la culture, le sport et les hobbies. Dans ce contexte, les sphères de pouvoir et d'influence suivantes sont brièvement présentées: propriété, participations, politique/militaire, associations, culture/sport, conseil/science. Deux personnes qui figuraient dans cette publication sans en avoir été informées nous ont priés d'intervenir auprès de l'éditeur des listes.
Les personnes privées n'ont pas le droit de communiquer à des tiers des données sensibles ou des profils de la personnalité sans motif justificatif. Nous entendons par profil de la personnalité une compilation d'un nombre important de données relatives à la structure de la personnalité, aux compétences et activités professionnelles, ou encore aux relations et activités extra-professionnelles qui donnent une image globale, ou une image partielle mais essentielle, de la personne concernée. Un

regroupement systématique des données, tel que nous venons de l'énumérer, offre une image partielle de la personne en cause.
En règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement à leur traitement. Les données contenues dans la publication n'ont pas toutes sans exception été rendues accessibles au public par les personnes concernées. Comme il ne semble pas y avoir d'intérêt public ou privé prépondérant à l'élaboration de telles listes, seul le consentement des personnes concernées peut constituer un motif justificatif pour le traitement. C'est pourquoi les personnes nouvellement enregistrées doivent en être formellement informées auparavant, afin qu'elles puissent donner leur accord au traitement et à la publication de leurs données.
Dans une note de bas de page de la publication, l'éditeur décline toute responsabilité pour l'exactitude des données publiées. Or, selon la LPD, le maître du fichier a l'obligation de s'assurer de ladite exactitude.
Pour ne pas annoncer ce fichier, le maître du fichier a invoqué l'article 10 LPD qui règle les restrictions du droit d'accès applicables aux médias, mais qui n'a rien à voir avec l'annonce de fichiers pour enregistrement, cette question étant réglée à l'article 4 OLPD. Or, selon cette disposition, ne sont pas soumis à déclaration les fichiers que le maître du fichier utilise exclusivement pour la publication dans la partie rédactionnelle d'un média à caractère périodique, et dont les données ne sont pas communiquées à l'insu des personnes concernées. Ce n'est toutefois pas le cas en l'espèce.
Quant aux personnes privées qui traitent régulièrement des profils de la personnalité ou communiquent des données à des tiers à l'insu des personnes concernées, elles ont l'obligation de nous annoncer leurs fichiers. Pour que l'obligation de déclaration tombe, les personnes concernées doivent connaître l'existence et l'identité du maître du fichier, un éventuel traitement de données sensibles ou de profils de la personnalité et une éventuelle communication à des tiers. Une annonce du fichier ne serait pas nécessaire dans le cas présent si le contenu ainsi que d'éventuels compléments ou modifications du portrait succinct avaient été communiqués à chaque personne concernée et si ces dernières consentaient expressément à une communication à des tiers. Pour ne pas devoir annoncer son fichier, l'éditeur de la publication a choisi cette manière de procéder.

7. Bulletin d'arrivée dans les hôtels

Toute personne logeant dans un hôtel ou dans une auberge doit en règle générale remplir un bulletin d'arrivée auprès de la réception. Ce formulaire contient des questions relatives aux nom, prénom, profession, date de naissance, nationalité, état civil, nombre d'enfants et numéro de passeport, mais également très souvent des questions relatives aux moyens de transport utilisés, lieu de provenance, date de départ, destination finale, etc.

Une personne concernée nous a demandé si elle était tenue de répondre à toutes les questions posées. Le traitement de données personnelles par des personnes privées tels que des hôteliers doit être effectué conformément à certains principes. La collecte des données doit être licite, c.-à-d. qu'elle doit se fonder sur une disposition légale, le consentement de la personne concernée ou être justifiée par un

intérêt public ou privé prépondérant. Elle ne doit en outre pas enfreindre des normes d'interdiction ou être effectuée par des moyens illicites tels que duperie ou menace.

La collecte de données par les logeurs repose en partie sur des obligations légales:

- ainsi une déclaration obligatoire est prévue pour les personnes logeant des étrangers moyennant rétribution, conformément à la Loi fédérale sur le séjour et l'établissement des étrangers ainsi que dans ses dispositions d'exécution. D'autre part, l'étranger est tenu de son côté de communiquer au logeur à l'intention des autorités des informations véridiques. Le logeur, lors de l'accomplissement de son obligation de déclaration, est tenu de veiller à ce que les informations fournies par l'étranger soient complètes et correctes. Il est en outre tenu de retirer les papiers d'identité de l'étranger lors de son arrivée et de les présenter à la police en même temps que le bulletin d'arrivée. Ceci a pour conséquence que les hôtels sont tenus d'utiliser des systèmes (de fiches de voyageurs ou autres) qui leur permettent de saisir les données nécessaires concernant leurs clients. L'obligation de déclaration réglementée dans ces ordonnances ne concerne cependant que les étrangers. Pour que les hôtels puissent identifier les étrangers, ils ont néanmoins besoin de connaître le nom, le prénom, l'adresse et la nationalité de tous leurs clients.
- L'Office fédéral de la statistique (OFS) établit une statistique hôtelière, conformément à la Loi sur la statistique fédérale. Cette statistique contient des enquêtes mensuelles concernant les arrivées et les nuitées des clients par pays de domicile. L'OFS est autorisé à vérifier les indications fournies par les personnes soumises à déclaration obligatoire, si nécessaire sur les lieux. Ces ordonnances ont donc également pour conséquence que les logeurs tiennent une comptabilité au sujet des personnes qu'elles ont logées, à l'aide d'un système de contrôle, que ce soit un simple livre des visiteurs ou un système de fiches de voyageurs.
- Finalement, certains textes légaux cantonaux relatifs à l'hôtellerie contiennent des dispositions relatives à l'obligation de déclaration des logeurs. En dehors des dispositions légales citées, le contrôle des clients incombe aux cantons. Ainsi chaque canton est en droit de décider de manière autonome quelles indications il requiert de la part des logeurs.

Ensuite, la collecte des données peut être justifiée par un intérêt prépondérant du logeur. Un tel intérêt peut entrer en considération lorsque les données sont traitées en rapport immédiat ou étroit avec la conclusion ou l'exécution d'un contrat. Ceci s'applique en tout cas aux informations dont le logeur a besoin pour pouvoir poursuivre le client au cas où celui-ci ne payerait pas sa facture. Le traitement des données personnelles doit en plus respecter le principe de la proportionnalité, c'est-à-dire que les données ne doivent être collectées que dans la mesure où elles sont absolument nécessaires au logeur pour assumer ses responsabilités et ses tâches.
Dans le cas où les logeurs sont obligés de par la loi de collecter les données, ils sont autorisés et tenus de demander les informations requises, et le client est obligé de répondre aux questions de manière complète et conforme à la vérité. Lorsque les informations demandées ne sont pas prescrites par la loi, le logeur est tenu de respecter le principe de la proportionnalité. Cela signifie qu'il ne peut demander que les informations dont il a vraiment besoin pour assumer ses devoirs dans le cadre du contrôle des clients. Afin que le logeur sache où il peut retrouver le client au cas où celui-ci ne tiendrait pas ses engagements, il a besoin au minimum de connaître les

nom, prénom, adresse exacte et nationalité de ce dernier ainsi que sa date de naissance, étant donné qu'il peut y avoir plusieurs personnes du même nom.

La réponse à la question de savoir quelles informations doivent être collectées par les logeurs et lesquelles doivent être fournies par les clients dépend donc d'une part des dispositions légales fédérales, d'autre part des dispositions cantonales relatives au contrôle des clients. L'appréciation de la mesure dans laquelle des collectes de données par le logeur sur la base des dispositions cantonales correspondent aux principes de la protection des données incombe aux organes cantonaux de contrôle de la protection des données .

8. Vignette de parcage

Un grand nombre d'entreprises et d'organes fédéraux offrent la possibilité à leurs collaborateurs de garer leurs véhicules sur des places de parc appartenant à l'entreprise ou louées à l'extérieur à cet effet. Les collaborateurs reçoivent à cette fin une vignette de parcage sous forme de carton à placer sur le tableau de bord ou sous forme d'étiquette à coller à l'intérieur du pare-brise.

Ces vignettes servent à indiquer lors d'un contrôle que le détenteur du véhicule est autorisé à utiliser une place de parc précise. Mises en rapport avec le véhicule auquel elles sont fixées, de telles vignettes se transforment en données personnelles étant donné qu'elles indiquent que le détenteur du véhicule est autorisé à utiliser la place de parc. Le détenteur du véhicule peut facilement être identifié d'après le numéro de plaque du véhicule. Les données visibles sur la vignette apposée au véhicule sont en règle générale accessibles à tout le monde.

Nous avons vérifié si l'utilisation de telles vignettes pouver donner lieu à des réclamations du point de vue de la protection des données. Il s'agissait surtout de vérifier si le principe de la proportionnalité était respecté. Les vignettes autocollantes ont été crées pour éviter que des personnes non autorisées puissent utiliser des autorisations de parcage, ce qui est possible lorsque les vignettes sont simplement posées sur le tableau de bord à l'intérieur du véhicule. L'utilisation de vignettes autocollantes peut donc être considérée comme proportionnelle. Le principe de la proportionnalité vaut également pour les données traitées et leur contenu. Ainsi, seules les données nécessaires pour atteindre le but fixé peuvent être traitées. Il n'est donc pas nécessaire pour le contrôle des véhicules garés que les vignettes contiennent des indications en langage clair sur l'employeur. Dans les cas où une personne travaille dans un domaine sensible tel que l'énergie nucléaire, une entreprise de pornographie, le Ministère public de la Confédération, une institution religieuse ou raciste, ces indications peuvent causer des désagréments ou même de sérieux ennuis au détenteur du véhicule. Une marque neutre ou une combinaison de lettres et de chiffres intelligibles uniquement par la personne chargée du contrôle suffit donc amplement à assurer le but de contrôle.

C'est pourquoi les vignettes de parcage doivent, conformément au principe de la proportionnalité (et, qui plus est, dans le cadre de contrats de travail privés conformément à l'article 328b CO; voir aussi pages 138 ss) être conçues de manière à ne pas contenir de données relatives à l'employeur déchiffrables par des tiers.

9. Communication de renseignements sur la durée de travail des chauffeurs de taxis

Une centrale de diffusion d'ordres de courses des taxis n'est tenue de fournir les renseignements nécessaires aux tâches de contrôle de l'autorité cantonale chargée de veiller à l'application des prescriptions fédérales et cantonales en matière de durée du travail et du repos des conducteurs professionnels, que dans la mesure où une disposition légale le prévoit.

En réponse à une demande d'un canton souhaitant connaître dans quelle mesure les centrales de diffusion d'ordres de courses étaient tenues de fournir les informations nécessaires aux tâches de contrôle de l'autorité cantonale chargée de veiller à l'application des prescriptions fédérales et cantonales en matière de durée du travail et du repos des conducteurs professionnels, nous avons souligné ce qui suit:
la communication de données personnelles à une autorité cantonale par une centrale de diffusion d'ordres de courses est soumise à la LPD dans la mesure où cette centrale est régie par le droit privé. Par contre les traitements de données personnelles effectués par les autorités cantonales chargées de l'application de prescriptions fédérales relèvent de la compétence cantonale. Ces organes ne sont régis par la loi fédérale sur la protection des données que s'ils traitent des données en exécution du droit fédéral et ne sont pas soumis à des dispositions cantonales de protection des données. Un canton dont la loi de protection des données ne couvrirait que les traitements automatisés serait par exemple soumis au droit fédéral lorsqu'il opèrerait un traitement manuel.
La centrale de diffusion n'est tenue de fournir aux autorités cantonales des données personnelles relatives aux chauffeurs de taxis et à leurs employeurs que si une disposition légale l'y contraint. Elle peut également le faire si les personnes concernées y ont consenti ou si elle peut faire valoir, dans un cas d'espèce, un autre motif justificatif (intérêt privé ou public prépondérant). La législation fédérale sur la circulation routière et sur la durée du travail et du repos des conducteurs professionnels de véhicules automobiles règle uniquement l'obligation de renseigner des employeurs et des conducteurs. Il en va de même de la législation cantonale régissant les entreprises de taxis. L'obligation de communication de données personnelles faite aux centrales de diffusion repose dès lors sur une base légale insuffisante. Elle ne peut finalement découler ni d'un intérêt public ou privé prépondérant dans la mesure où elle revêt un caractère systématique et régulier, ni d'un autre motif justificatif admis par la LPD.

10. Repérage électronique

L'informatique et notamment la technologie de la puce électronique permettent aujourd'hui de développer des techniques de repérage des véhicules, en particulier aux fins de retrouver des véhicules volés ou de faciliter les opérations de péage sur les autoroutes ou aux passages alpins. Le recours à ces technologies, avons-nous relevé, ne doit pas se faire au détriment de la protection des données. L'utilisation de ces systèmes doit être limitée à des finalités bien déterminées (par ex., repérage d'un véhicule volé, péage routier). Les systèmes retenus doivent garantir, autant que faire ce peut, l'anonymat des usagers. Nous avons finalement souligné que les potentialités multifonctionnelles offertes par ces technologies ne sont pas sans

risque pour le respect des droits fondamentaux des individus et peuvent déboucher sur l'instauration d'une société sous surveillance électronique.

L'informatique et la télématique apparaissent de plus en plus dans la gestion des transports et de nos déplacements que ce soit pour contrôler le trafic, faciliter la fluidité, éliminer les files d'attente aux péages, intercepter les véhicules en faute ou retrouver des véhicules accidentés, disparus ou volés, etc. En Suisse, ces technologies commencent également à faire leur apparition, et nous avons été appelés à nous prononcer sur deux applications qui sont encore à l'étude: le recours à un système informatique pour la perception de taxes sur les passages alpins et l'introduction d'une puce électronique dans le but de repérer les véhicules volés.
Un groupe de travail présidé par l'OFP étudie actuellement l'introduction d'un système permettant la perception des taxes sur les passages alpins suite à l'acceptation par le peuple de l'initiative sur les Alpes. La mise en place et l'exploitation de moyens techniques pour la perception de taxes sont soumises à la LPD, dans la mesure où elles génèrent un traitement de données personnelles. Ceci implique notamment que le traitement doit reposer sur une base légale suffisante et respecter les principes généraux de traitement. Il y aura lieu de tenir spécialement compte des principes de proportionnalité et de finalité. On retiendra ainsi un système qui, tout en permettant de prélever la taxe en assurant la fluidité et la sécurité du trafic tout en préservant l'environnement et l'aménagement du territoire, porte le moins atteinte à la personnalité et aux droits fondamentaux des personnes concernées (détenteur du véhicule, conducteur ou passagers). On préférera par exemple à la carte à "postpaiement", impliquant la collecte et le traitement de données personnelles, la vignette ou la carte à prépaiement, garantes de l'anonymat des utilisateurs. Si un système à postpaiement doit néanmoins être retenu, la collecte de données se limitera aux seules informations nécessaires au prélèvement de la taxe (en particulier identification du véhicule, lieu, date et heure de passage, nom et adresse du détenteur ou de la personne chargée de s'acquitter de la taxe, montant de la taxe). Les données recueillies ne seront utilisées qu'à cette fin et seront détruites une fois le montant de la taxe acquitté. L'introduction du système de prélèvement de la taxe pourrait être accompagnée de mesures techniques (appareil photographique ou caméra vidéo) permettant d'enregistrer les véhicules ne s'étant pas acquittés de leur dû. Dans ce cas également, il conviendra d'éviter que ces informations soient utilisées à d'autres fins et en particulier que des informations sur les personnes ayant rempli leurs obligations soient enregistrées et conservées. Le système devra être conçu de manière à ne pas pouvoir être utilisé en violation des règles de protection des données.
Nous avons examiné une seconde application qui permet de détecter et de retrouver les véhicules volés, ainsi que d'exercer un télégardiennage des voitures. Ce système déjà introduit en France devrait être commercialisé en Suisse cette année encore. Il implique en particulier l'installation d'une puce électronique précodée et pratiquement indétectable dissimulée dans la voiture. Cette puce permet d'établir la connexion avec un système d'informations automatisé. En outre, le réseau routier doit être équipé de sites de détection placés à des endroits stratégiques (carrefour, entrée et sortie de garages ou de stations services, entrée ou sortie d'autoroute, etc.). Le système de détection n'est sensé se déclencher que dans la mesure où un véhicule est déclaré volé. Le véhicule une fois repéré, l'information, à savoir les date, heure, lieu de repérage, destination présumée, marque de la voiture, modèle, genre, couleur et numéro d'immatriculation, est transmise par fax ou téléphone à la police qui peut intervenir et intercepter le véhicule et le voleur. Une fois ce système introduit

en Suisse, les codes confidentiels et les spécifications des véhicules déclarés volés pourront être transmis aux sociétés gérant le système dans d'autres pays afin de leur permettre de télécharger leur propre réseau de détection avec ces informations. Les personnes intéressées concluent un contrat avec la société gérant le système. Cela nécessite la collecte et le traitement de données personnelles: nom, prénom, adresse complète, véhicule (marque, modèle, numéro d'immatriculation, numéro de série, numéro de la police d'assurance, assurance), mode de règlement (compte bancaire, chèque, espèce), autorisation de prélèvement pour le renouvellement de l'abonnement (établissement bancaire, adresse, numéro de compte), nom du club automobile auquel la personne concernée est éventuellement affiliée et nom de l'assurance du véhicule.
Lors de l'examen du système projeté, nous avons constaté que dans la mesure où son introduction est envisagée sur une base contractuelle, uniquement aux fins de repérage des véhicules volés ou suspectés de l'être (télégardiennage), et si seules les données nécessaires à retrouver le véhicule et à intercepter le voleur seront le cas échéant communiquées à la police, ce système ne portera pas une atteinte illicite à la personnalité des personnes concernées. Toutefois le traitement devra se faire dans le respect des principes généraux de traitement des données, notamment des principes de proportionnalité, de finalité et de sécurité des données et garantir le respect des droits des personnes concernées. Ceci implique en particulier que:

- la collecte et le traitement de données interviendront avec le consentement exprès et éclairé de la personne concernée. Celle-ci aura connaissance des données traitées, des finalités du traitement et de l'existence des fichiers nécessaires à l'exécution du contrat;
- seules les données nécessaires à la conclusion et à l'exécution du contrat seront traitées. Le catalogue retenu n'est en l'espèce pas excessif;
- les données ne seront pas conservées au-delà de ce qui est nécessaire à l'exécution du contrat. C'est ainsi que les passages de véhicules non volés ou non suspects d'avoir été volés (télégardiennage) ne seront pas enregistrés. A l'échéance du contrat, les données personnelles seront détruites une fois les délais légaux de conservation échus, et la puce sera désactivée et si possible enlevée du véhicule;
- les données sur les véhicules volés seront communiquées uniquement à la police pour lui permettre de retrouver les véhicules rapidement et ne seront utilisées par celle-ci qu'à cette fin. La personne concernée sera informée de cette communication lors de la conclusion du contrat, mais au plus tard lors de la survenance d'un vol. Lors du télégardiennage, la personne concernée sera informée si son véhicule est déplacé de manière suspecte afin qu'elle puisse en cas d'erreur stopper la procédure. Tous autres traitement et communication à la police et à d'autres autorités ne seraient pas couverts par le motif justificatif (exécution du contrat) et porteraient une atteinte illicite à la personnalité des personnes concernées. D'éventuelles utilisations ultérieures par les autorités ou une généralisation du système sous forme d'obligation devraient reposer sur une base légale suffisante et être précédées d'une analyse détaillée des besoins.

11. Nom et adresse de détenteurs de véhicules par le biais du numéro 111 et du vidéotex

La communication de l'identité de détenteurs de véhicules à moteur par l'intermédiaire du 111 ou du vidéotex est conforme à la législation fédérale sur la circulation routière dans la mesure où seul un renseignement par appel et par numéro de plaque de contrôle est donné et si seuls les nom, prénom et adresse du détenteur sont communiqués. Les données communiquées ne doivent être utilisées qu'à des fins qui sont en rapport avec la circulation routière. Les détenteurs de véhicules doivent pouvoir s'opposer à la communication et à la publication de leur identité.

Toute personne qui circule au volant d'un véhicule automobile n'est pas sans autre identifiable pour les autres usagers de la voie publique. D'après la législation en vigueur en matière de circulation routière, le véhicule doit être identifiable par l'intermédiaire du numéro d'immatriculation. Les occupants d'un véhicule autres que le détenteur n'ont pas à s'identifier sans motifs. Il n'est également pas nécessaire d'identifier le détenteur d'un véhicule qui a un comportement conforme aux exigences légales. Ce n'est qu'en cas de perturbation, d'incidents graves ou d'accidents que la question de l'identification se pose. Même à bord d'un véhicule automobile circulant sur la voie publique, l'individu a droit au respect de sa vie privée. Pour éviter qu'une communication de données ne serve qu'à assouvir la curiosité et que ces données soient utilisées à des fins incompatibles avec la loi, notamment afin de nuire au détenteur ou à ses proches, l'octroi de renseignements devrait dépendre de la justification d'un intérêt (par ex. implication du détenteur dans un accident, perturbation du trafic, mise en danger). Or cela nécessiterait une modification préalable de la législation.
En vertu de la loi fédérale sur la circulation routière, les cantons sont compétents pour collecter et traiter les données personnelles relatives aux détenteurs de véhicules à moteur. La loi leur confère également la faculté de publier la liste des détenteurs. En outre, indépendamment de l'existence d'une telle publication, les offices cantonaux de la circulation renseignent par téléphone les personnes qui souhaitent connaître l'identité d'un détenteur de véhicule. Depuis l'année dernière, en raison de la surcharge de travail de ses membres et pour améliorer le degré d'actualité des répertoires, l'Association des services automobiles a confié aux PTT la tâche de renseigner les personnes qui le demandent. Pour ce faire, les PTT reçoivent des cantons le numéro de la plaque de contrôle, ainsi que les nom et adresse du détenteur de véhicule. Les renseignements sont fournis par l'intermédiaire du 111 et du vidéotex. La décision de publier la liste des détenteurs ou de recourir aux PTT incombe uniquement aux cantons.
La publication et la communication des renseignements sont régis par la législation fédérale sur la circulation routière et par les lois cantonales de protection des données. Dans la mesure où un canton n'est pas soumis à des dispositions cantonales de protection des données, la LPD s'applique. Consultés par l'Office fédéral de la police, l'Association des services automobiles et certains cantons, nous avons émis certaines réserves quant à la nécessité et à l'opportunité de la publication d'annuaires sur les détenteurs de véhicules et à leur diffusion par le biais du 111 ou du vidéotex. Nous avons insisté sur la nécessité de ne donner accès à l'information que par l'intermédiaire du numéro d'immatriculation et de s'en tenir aux dispositions idoines de la législation fédérale sur la circulation routière limitant la communication aux nom, prénom et adresse du détenteur. Ceci implique que la

communication intervient dans un cas d'espèce (un renseignement par appel) et non de manière systématique et régulière, et qu'elle respecte les finalités de la législation sur la circulation routière.
Nous avons au demeurant souligné qu'il est exclu de délivrer par le biais du 111 ou du vidéotex des listes, d'utiliser d'autres critères de recherche que le numéro d'immatriculation ou d'étendre le catalogue de données à la date de naissance, à la nationalité, au canton d'origine ou à l'identité de l'assurance responsabilité-civile du détenteur.
La législation fédérale permet néanmoins aux autorités compétentes en matière de circulation routière de révéler sur demande l'identité de l'assureur aux personnes impliquées dans un accident ou lors d'un changement de détenteur. En outre d'autres renseignements tirés du permis de circulation peuvent être communiqués, sur demande écrite et motivée, aux personnes qui font valoir un intérêt suffisant, en vue d'une procédure.
La publication et la communication de l'identité du détenteur n'étant pas obligatoires, celui-ci doit pouvoir s'opposer à la communication et/ou à la publication. Le droit d'opposition est régi par le droit cantonal. Nous avons constaté de grandes disparités dans l'application de ce droit. Certains cantons refusent systématiquement de bloquer les données ou mettent des conditions très élevées, alors que d'autres cantons ne font dépendre l'exercice de ce droit d'aucune condition. Il serait souhaitable que les cantons ne soient pas plus restrictifs que la loi fédérale sur la protection des données et admettent l'opposition dès le moment où le détenteur rend vraisemblable un intérêt légitime. Ainsi l'opposition à la publication ou à la communication devra être acceptée si l'autorité ne peut manifestement pas exclure que la communication de données puisse entraîner une atteinte à la liberté personnelle ou à la personnalité de la personne concernée.

12. Système d'archivage des caisses de chômage

Depuis quelques années, les caisses de chômage sont confrontées à un volume de travail croissant. En collaboration avec l'Office fédéral de l'industrie, des arts et métiers et du travail (OFIAMT), les caisses de chômage de Suisse romande ont lancé un projet-pilote de mise sur microfilm des dossiers afin de gérer et surtout d'archiver de manière rationnelle les dossiers qui s'amoncellent. Nous avons contrôlé les mesures requises pour que ce projet soit réalisé conformément à la protection des données.

L'OFIAMT a approuvé la constitution d'un centre de microfilmage permettant aux caisses cantonales de chômage de gérer rationnellement le volume considérable de dossiers à archiver. Ce centre sera intégré au Centre de formation des caisses de chômage romandes de La Chaux-de-Fonds. Dans une première phase, le projet-pilote prévoit la mise sur microfilm des dossiers de toutes les caisses de chômage de Suisse romande. Au cours de la seconde phase, le centre traitera tous les dossiers archivés de toutes les caisses suisses de chômage.

Ce processus de rationalisation impliquera le traitement de données personnelles en ce sens qu'elles seront archivées et filmées. En tant que mesures d'aide sociale, les données sur les chômeurs constituent des données sensibles au sens de l'article 3 lettre c chiffre 3 LPD. Un traitement illicite de ces données porterait donc une atteinte très grave à la personnalité des citoyens concernés. L'OFIAMT nous a priés

d'examiner les conditions à remplir pour que le traitement de ces données soit conforme à la loi. Au terme de quelques séances, nous avons recommandé à l'OFIAMT de créer les bases légales nécessaires au traitement de ces données et d'arrêter les mesures techniques et organisationnelles indispensables à la protection des données.

13. TVA et secret professionnel

Appelés à donner notre avis suite à deux interpellations parlementaires relatives à l'obligation des avocats de révéler l'identité de leurs clients domiciliés à l'étranger pour bénéficier d'une exonération de la TVA, nous avons conclu qu'un avocat ne devrait être tenu de donner les renseignements demandés par les autorités fiscales que dans la mesure où les clients y ont préalablement consenti et si la preuve du droit à l'exonération fiscale ne peut être apportée autrement.

La législation sur l'impôt fédéral sur la valeur ajoutée (TVA) exonère de l'impôt les prestations de services qui sont effectuées à l'étranger. Sont en particulier concernés par cette exonération les avocats dont les clients sont domiciliés ou ont leur siège social à l'étranger pour autant que les prestations fournies ne soient utilisées qu'à l'étranger. Pour en bénéficier, l'avocat doit prouver le droit à l'exonération en fournissant des documents comptables et des pièces justificatives. Les bénéficiaires de l'exonération sont à la fois l'avocat qui fournit la prestation et le client qui ne se verra pas facturer la TVA. Pour obtenir l'exonération, l'avocat doit fournir à l'administration fiscale des informations relatives au client, en particulier ses nom et adresse. Consultés au sujet de la réponse à apporter à deux interventions parlementaires dans lesquelles était soulevée la question de la conformité de cette obligation au secret professionnel des avocats, nous avons émis l'avis suivant:

la législation fédérale sur la TVA impose à tout assujetti une obligation d'informer les autorités sur tous les faits qui peuvent avoir de l'importance pour la constatation de l'assujettissement ou le calcul de l'impôt. Elle prévoit également l'obligation de conserver certains documents de manière à pouvoir déterminer l'assujettissement ou l'exonération. Elle confère à l'administration fiscale une compétence de contrôle. Enfin, elle donne la faculté à l'administration fiscale de demander des renseignements à des tiers et notamment à des personnes ayant reçu ou effectué des prestations de services. Elle ne précise cependant pas quelles données personnelles relatives à des tiers peuvent être requises. Le respect du secret professionnel demeure garanti. Cette garantie du secret professionnel s'applique à l'avocat appelé à fournir le nom et l'adresse de son client, lequel est le véritable bénéficiaire de l'exonération.
L'obligation de fournir les nom et adresse du bénéficiaire d'une prestation soumise à exonération implique un traitement de données personnelles par un organe fédéral. Il est régi par la LPD et doit notamment reposer sur une base légale et respecter les principes généraux de traitement. Dans le cas d'espèce, la base légale existe, mais l'ordonnance sur la TVA est insuffisante pour lever un secret professionnel protégé par une loi au sens formel. La communication par l'avocat des informations demandées ne peut dès lors intervenir qu'avec le consentement de la personne concernée. En outre avant de généraliser une telle obligation, il y aurait lieu d'examiner si les nom et adresse du bénéficiaire d'une prestation à l'étranger sont toujours nécessaires à la preuve du bien-fondé de l'exonération ou s'il n'est pas possible de demander ces données uniquement en cas de doute ou lors d'un

contrôle. En effet, si l'avocat est en mesure d'apporter la preuve du droit à l'exonération sans communiquer de données personnelles, l'obligation d'informer doit tomber. Enfin si l'avocat est appelé à donner des informations et que son client refuse son consentement, il informera ce dernier des conséquences possibles de ce refus, à savoir le risque de devoir s'acquitter du paiement de l'impôt.

14. Casinos - avant-projet provisoire de loi fédérale

Le Département fédéral de justice et police a institué une Commission d'experts dénommée "Loi sur les casinos". En septembre 1994, l'Office fédéral de la police, chargé de la rédaction d'un avant-projet de loi fédérale sur les casinos devant servir de base de travail aux délibérations de la Commission d'experts, nous a transmis un document provisoire en nous priant de procéder à un examen sommaire de sa conformité aux exigences de la protection des données, avant que ne soit ouverte la procédure de consultation officielle.

Dans le cadre de notre prise de position, nous avons attiré l'attention des experts sur le fait que de manière générale, la mise en place de cette législation sur les casinos devait notamment respecter les principes généraux de la loi fédérale sur la protection des données. A ce stade de l'avant-projet provisoire, il nous était cependant extrêmement difficile d'évaluer si ces principes étaient respectés, en particulier le principe de la proportionnalité. En effet, aucun commentaire ou rapport explicatif n'avait encore été élaboré, afin de justifier la tenue des registres prévus pour la gestion des casinos, soit le registre de données personnelles d'identification des joueurs, le registre de données personnelles sur les exclusions des personnes interdites de jeux ou encore le registre de données personnelles sur les transactions. Nous avons en outre rappelé que le contenu de ces registres devra également répondre au critère de proportionnalité afin que seules les données personnelles nécessaires soient collectées et enregistrées.

Un certain nombre d'observations spécifiques à quelques dispositions de l'avant-projet provisoire ont également été émises par nos soins, et ce afin de répertorier, à l'attention de la Commission d'experts, certains points problématiques sous l'angle de la protection des données. Nous avons notamment relevé que des précisions devaient être apportées quant aux données relatives à l'identité (''Personalien'') et aux durées de conservation. Nous avons également recommandé d'assortir le devoir de communication en faveur des autorités de poursuite pénale et de l'Office fédéral de la police d'une interdiction, pour le gérant d'un casino, d'enregistrer les soupçons qu'il a portés contre un joueur et qu'il a annoncés à ces autorités.
Il a en outre été souligné que le droit d'accès de la personne concernée peut être exercé sur l'ensemble des données la concernant enregistrées par le gérant d'un casino, et que ce droit est en principe gratuit. Les exceptions à la gratuité des renseignements sont prévues dans l'ordonnance relative à la loi fédérale sur la protection des données. Pour ce qui concerne la prévention de l'endettement, la disposition y relative devra être complétée afin d'éviter ou d'interdire la mise en place d'enquêtes ou de collectes abusives de données par les gérants de casinos dans le cadre de l'application de cette norme à caractère social. Enfin, nous avons recommandé d'examiner, sous l'angle de l'opportunité et de la proportionnalité, la question de la communication des interdictions de jeux (mesures d'exclusion) à tous les autres casinos de Suisse. Le cas échéant, la réglementation devrait prévoir le

mode de communication et un mécanisme de mise à jour en cas d'annulation de l'interdiction.
Les experts ont été invités à porter toute leur attention sur nos observations, tout en tenant compte du fait que nos considérations n'avaient pu être développées que dans le cadre d'un examen sommaire de l'avant-projet provisoire. Certaines observations devront encore être approfondies ou éventuellement revues, principalement sous l'angle du principe de la proportionnalité, lors de la procédure de consultation des offices, lorsque le rapport explicatif contenant les commentaires relatifs à chaque disposition aura été élaboré.
La version finale de l'avant-projet de loi fédérale sur les casinos nous a été adressée dans le cadre de la procédure de consultation des offices ouverte fin janvier 1995. Un nouvel examen de ce projet législatif est en cours pour une éventuelle prise de position complémentaire.

15. Assujettissement à la loi fédérale sur la protection des données

Le tiers qui traite des données personnelles pour le compte d'une entreprise privée ou d'un organe fédéral demeure soumis à la loi fédérale sur la protection des données.

Une société de services, dont le siège est en Suisse, traite pour le compte d'entreprises commerciales et industrielles des données personnelles relatives à la gestion et au salaire du personnel de ces entreprises. Les données sont en grande partie traitées sur un centre de calcul situé en France. La société intervient en tant que mandataire et ne détient pas les fichiers des données du personnel de ses mandantes. Consultés sur la question de savoir si cette société était néanmoins soumise à la LPD, nous avons relevé ce qui suit:

toute personne physique ou morale qui traite des données personnelles en Suisse est soumise aux obligations qui découlent de la LPD, peu importe qu'elle intervienne en tant que maître d'un fichier, mandataire ou à un autre titre. La loi précise en particulier que la personne qui charge un tiers d'un traitement de données personnelles doit veiller à ce que ce tiers se conforme aux impératifs de la protection des données dans la même mesure qu'elle-même y est tenue. Cela concerne toutes les formes de traitement, de la collecte des données à leur communication, conservation ou destruction. Le mandataire peut faire valoir les mêmes motifs justificatifs que le mandant.
Toutefois, sous réserve d'une disposition légale ou contractuelle contraire, le mandataire n'est pas tenu de s'acquitter des éventuelles obligations d'annonce des fichiers et des flux transfrontières de données qui incombent au maître du fichier. Lorsqu'une personne concernée fait usage de son droit d'accès et s'adresse au mandataire, celui-ci n'est tenu de communiquer les renseignements demandés que s'il ne révèle pas l'identité du maître du fichier ou si ce dernier n'a pas de domicile en Suisse. La personne concernée qui se prétend atteinte dans sa personnalité peut actionner non seulement le maître du fichier, mais également le mandataire chargé du traitement.

16. L'application de mesures de sécurité des données dans l'administration fédérale

Dans de nombreux cas, les dossiers de projets qui nous sont remis sont incomplets. Souvent les processus (organisation fonctionnelle) et la configuration des moyens informatiques ne sont pas mentionnés ou le sont de manière incomplète, ou alors les mesures de protection des données ne sont pas décrites de manière suffisamment détaillée.

Les expériences faites lors de l'application des mesures techniques et organisationnelles de la protection des données sont très variées. Alors que certaines unités de gestion prennent très au sérieux les préoccupations de la protection des données, d'autres modifient leurs systèmes ou en développent de nouveaux sans tenir compte suffisamment des contraintes. Les exigences de la protection des données doivent être immédiatement prises en compte et appliquées lors d'un nouveau développement ainsi que lors d'une modification de systèmes. La période transitoire de 5 ans (jusqu'au 1er juillet 1998) pour l'application des mesures techniques et organisationnelles ne vaut que pour les systèmes qui étaient déjà en service au 1er juillet 1993 et auxquels on n'a pas apporté de modifications "majeures".
Les dispositions techniques pour protéger les données personnelles nécessitent un effort particulier. Cet effort ne doit pas être sous-estimé, surtout si par le passé les points de vue organisationnels ainsi que les aspects relatifs à la sécurité des données n'ont pas été suffisamment pris en compte. Le plus important est que les processus soient documentés (ordinogrammes) et que l'organisation structurelle soit définie (qui est compétent pour quelle tâche?). Ces exigences de la protection des données ne sont pas nouvelles, elles sont également requises par exemple par l'assurance qualité ou dans l'optique de l'organisation. La complexité des mesures de sécurité des données dépend du système. C'est pourquoi la mise en oeuvre de ces mesures devrait toujours se faire aussi rapidement que possible. Pour être à même de prendre une décision concernant les mesures de sécurité des données, il faut avoir une vue d'ensemble du système. Ceci nécessite qu'on indique la configuration des moyens informatiques, dans la mesure où ceux-ci jouent un rôle pour la protection et la sécurité des données. Ce n'est que sur la base de ces documents que l'on peut fixer quelles sont les mesures de sécurité à prendre et constater si les risques peuvent être raisonnablement couverts.

La responsabilité de la protection des données et donc de la sécurité des données incombe au maître de fichier. Souvent, ce dernier n'est pas en mesure de s'initier de manière approfondie aux domaines de l'informatique, de la gestion d'entreprise (organisation) et du droit, pour être en mesure d'évaluer quelles sont les mesures qui s'imposent. Il dépend donc d'une assistance de la part des conseillers en matière de protection des données et des chargés de sécurité auprès des départements et des offices (dans la mesure où ils existent) ainsi que de la section "Sécurité" de l'Office fédéral de l'informatique. Ces derniers ont le devoir d'informer le maître de fichiers sur les mesures possibles et leurs conséquences ainsi que sur les ressources nécessaires, afin qu'il soit en mesure de choisir une solution appropriée pour le système en question. La solution doit en particulier être appropriée en ce qui concerne la protection de la personne concernée. Les coûts ne jouent dans ce cas qu'un rôle secondaire. Le maître de fichier décide si la solution est appropriée et porte la responsabilité de la protection des données. Des détails relatifs aux mesures

possibles sont donnés dans le *Guide relatif aux mesures techniques et organisationnelles de la protection des données*, qui peut être obtenu gratuitement auprès de notre Secrétariat. Si les exigences de la protection des données ne sont pas suffisamment prises en compte au niveau technique et organisationnel, ceci peut avoir pour conséquence une recommandation de la part du Préposé fédéral à la protection des données.
Il reste à souhaiter que les exigences de la protection des données soient à l'avenir mieux prises en considération lors de nouveaux développements ou de modifications de systèmes de traitement de données personnelles.

17. Communication non autorisée de données à des tiers par les organes fédéraux

Si un organe fédéral transmet, sans y être autorisé, des données à des tiers, les personnes lésées de ce fait dans leur personnalité peuvent exiger de l'organe fédéral en cause que le caractère illicite du traitement soit constaté. Une décision négative de cet organe peut être portée devant la Commission fédérale de la protection des données.

Dans le cas présent, plus de vingt personnes privées s'étaient rassemblées pour créer une entreprise en commun. Afin de donner plus de poids à une requête en rapport avec la création de l'entreprise, une liste de tous les participants avec leur signature a été soumise à l'organe fédéral compétent. Or, plusieurs requêtes similaires d'autres personnes avaient déjà été déposées auprès de cet organe. Parmi elles se trouvait aussi une requête de l'employeur d'une des personnes privées participant à la fondation de l'entreprise susmentionnée. La liste complète des signatures avait été remise à cet employeur "dans l'intérêt d'une meilleure coordination", alors même que sur la liste figurait l'interdiction formelle d'une quelconque communication à des tiers. Suite à cette communication, la personne engagée chez l'employeur en question perdit son emploi. Elle s'adressa à nous pour nous demander conseil.

En principe, les organes fédéraux ne sont en droit de communiquer des données personnelles que s'il existe une base juridique au sens de l'art. 17 LPD ou si la personne concernée a rendu ses données accessibles à tout un chacun (article 19, 1er alinéa, lettre c, LPD). Dans le cas présent, aucune base juridique ne prévoyait une communication de données personnelles à des tiers. Et comme les personnes en cause avaient en outre formellement interdit la communication de leurs données à des tiers, celle-ci ne peut être admise et le traitement des données doit être considéré comme illicite. Nous avons sommé l'organe fédéral de ne plus procéder à l'avenir à de telles communications de données.
Pour sa part, la personne concernée peut exiger de l'organe fédéral qu'il constate le caractère illicite du traitement de données. Si un dommage en a résulté, la personne concernée doit faire valoir ses droits dans l'année qui suit la connaissance dudit dommage et prouver ce dernier.
Si l'organe fédéral conteste le caractère illicite, on peut faire appel à la Commission fédérale de la protection des données dont la décision peut faire l'objet d'un recours de droit administratif auprès du Tribunal fédéral.

18. Recrutement - questionnaire médical

Avant le recrutement, tous les conscrits doivent remplir un questionnaire médical. Il ne s'agit pas uniquement de questions relatives à la santé de la personne en cause, mais aussi de questions sur les membres de sa famille. Dans le cadre de la réforme Armée 95, il importe de contrôler dans quelle mesure toutes ces questions sont encore nécessaires et opportunes.

Le père d'un conscrit s'est adressé à nous à ce propos. Il voulait savoir si toutes les questions sur les parents, les frères et soeurs, ainsi que sur le conscrit lui-même sont effectivement nécessaires. Le questionnaire porte, entre autres, sur les dates de naissance des parents et des frères et soeurs, sur leurs maladies, leurs causes de décès et années de décès, ainsi que sur la profession du père. Il est également demandé où le conscrit a grandi. Le questionnaire médical est utilisé par l'Office fédéral des affaires sanitaires de l'armée lors de la conscription des futures recrues. Il sert avant tout à la rationalisation de la procédure, permettant ainsi d'éviter l'interrogation systématique de chaque individu. Sur la base des antécédents, de la documentation médicale apportée et des résultats des examens médicaux, il est possible de constater si les conscrits sont aptes au service militaire. Mais il n'existe jusqu'à présent pas de base légale pour la récolte des données. Après le recrutement, les données recueillies ne sont disponibles que pour les médecins militaires et l'assurance militaire; elles ne sont pas exploitées systématiquement.

Une refonte du questionnaire médical est également prévue dans le cadre de la révision des prescriptions et formulaires. Il faudra examiner dans ce contexte lesquelles de ces indications sont aujourd'hui encore utiles et pertinentes, et si l'on peut partiellement y renoncer. En outre, il sera nécessaire d'élaborer une base légale pour la collecte de ces données.

19. Protection des données dans les secteurs du droit fiscal et du registre foncier

Même si les cantons gèrent des banques décentralisées de données, des concepts toujours plus vastes de protection et de sécurité des données s'avèrent de plus en plus judicieux. Cet objectif a été bien reconnu dans l'ordonnance révisée sur le registre foncier.

Aussi bien dans le secteur du droit fiscal que dans celui du droit du registre foncier, les données acquises pour accomplir les tâches de la Confédération sont traitées de manière décentralisée par les cantons. Ces derniers ont du reste de plus en plus recours aux moyens TED; le code civil révisé et l'ordonnance révisée sur le registre foncier les y autorisent pour le registre foncier. Pour le moment, il n'existe pas de prescriptions comparables dans le secteur du droit fiscal.

L'exigence de ce développement consiste à choisir, lors de l'utilisation du TED, des solutions compatibles avec la protection des données, mais également respectueuses de la souveraineté cantonale. Ces solutions doivent en outre être à même de remplir les exigences multiples des offices fédéraux concernés et autres utilisateurs des fichiers dont il est question, ainsi que de la protection de la personnalité ou d'éventuels intérêts justifiés de maintien du secret des personnes concernées. Avec

ses prescriptions relatives à la sécurité des données et à l'obligation d'élaborer des concepts de sécurité et de les soumettre à un examen préalable externe, ainsi que ses règles relatives aux accès par procédure d'appel et à leur étendue, le chapitre de l'ordonnance du registre foncier sur le registre foncier informatisé présente un intérêt particulier. Ces prescriptions ou des normes similaires pourraient également s'avérer judicieuses en droit fiscal.

III. ACTIVITES INTERNATIONALES

1. Conférence Internationale des Commissaires à la protection des données

Les instances chargées de veiller à l'application des dispositions nationales de protection des données ont institué une conférence internationale qui se réunit une fois l'an sur invitation de l'un des Etats-membres. Cette conférence a pour but d'échanger des informations entre autorités de contrôle, de consolider et d'harmoniser les pratiques, et le cas échéant d'adopter des positions communes sous forme de déclaration ou de résolution. La conférence est en partie ouverte et accueille des représentants des milieux concernés par l'application des dispositions de protection des données.

La XVIe Conférence Internationale des Commissaires à la protection des données s'est déroulée à La Haye du 6 au 8 septembre 1994, à l'invitation du commissaire néerlandais. La Conférence était placée sous le signe des nouvelles technologies de l'information et a notamment permis d'analyser les avantages de l'émergence de technologies de la vie privée. Réunissant des représentants venant de toutes les parties du monde, la Conférence a permis de faire le point sur le développement international de la protection des données. Elle a également été l'occasion d'un échange approfondi sur les traitements de données dans le domaine financier et notamment l'appréciation de crédit (recours à la technique du score permettant de dresser des profils de la personnalité par enrichissements et comparaisons de fichiers en vue notamment de procurer une aide à la décision), dans le domaine de la santé et sur l'évolution des nouvelles technologies de l'information (multimédias, autoroutes de l'information, Internet, cartes à puce notamment en matière de transports ou de santé) qui ne connaissent plus de frontières et qui engendrent de nouveaux défis pour le respect de la personnalité et des droits fondamentaux. Il est ainsi apparu nécessaire de promouvoir des technologies permettant d'assurer le respect de la protection des données, notamment en recourant à des techniques d'encryptage, en favorisant des technologies garantissant l'anonymat (cartes à prépaiement) ou encore limitant les accès aux données en fonction des utilisateurs et des finalités poursuivies. Les commissaires ont également mis l'accent sur la nécessité de renforcer la collaboration internationale et de mieux faire connaître la protection des données notamment en développant des politiques d'information du citoyen.

En complément à la Conférence annuelle, les commissaires collaborent entre eux, soit de manière bilatérale (échange d'informations), soit en constituant des groupes de travail sur des questions particulières. Tel est le cas du groupe de Berlin qui se

réunit deux fois par année pour examiner les problèmes de protection des données dans le domaine des télécommunications et des médias. Ce groupe se penche actuellement sur le réseau Internet qui permet de diffuser à travers le monde des données personnelles sans difficultés particulières. Ce réseau pose de gros problèmes de protection des données du fait de l'absence de dispositions légales équivalentes et d'instance spécifique de contrôle. Il examine également l'utilisation des télécommunications dans les relations de travail, les cartes téléphoniques, les annuaires électroniques et la surveillance électronique des détenus. Celle-ci constitue une alternative à la prison en permettant de suivre les mouvements d'un détenu et de lui fixer des limites dans ses activités et ses déplacements.

2. Conseil de l'Europe

L'activité internationale du préposé fédéral à la protection des données se concentre pour une part importante dans le suivi des travaux du Conseil de l'Europe. Cette instance joue un rôle fondamental dans le développement du droit de la protection des données en Europe et sa Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) a déjà été ratifiée par 16 Etats-membres, à savoir l'ensemble des Etats ayant adopté une loi de protection des données, à l'exception de la Suisse. Sur mandat du DFJP, nous nous sommes attelés à la préparation du message en vue de la ratification et nous espérons que la Suisse adhérera à ce traité au début de la prochaine législature.
Les deux comités chargés des questions de protection des données ont poursuivi leurs travaux. Ainsi, le Groupe de projet sur la protection des données (CJ-PD) s'est réuni à deux reprises et a finalisé deux recommandations. Tout d'abord la recommandation sur la protection des données à caractère personnel dans le domaine des services de télécommunication eu égard notamment aux services téléphoniques, adoptée par le Comité des Ministres dans sa séance des 6 et 7 février 1995. Cette recommandation dégage en particulier des règles applicables aux annuaires, à l'utilisation des données à des fins de marketing direct, à la facturation détaillée, à la téléphonie interne, à l'identification de la ligne d'appel, au transfert d'appels et à la téléphonie mobile. Ensuite, la recommandation relative à la protection des données médicales, dont l'adoption par le Comité des Ministres a été différée pour permettre au Comité de la santé publique de donner son avis. Cette recommandation s'appliquera à tout traitement de données médicales, qu'il intervienne dans le domaine de la santé ou dans un autre contexte, qu'il soit le fait d'un médecin ou d'une autre personne. Elle couvre également la recherche médicale et les données génétiques. La recommandation contient notamment des règles qui renforcent la confidentialité lors du traitement de données médicales, garantissent à la personne concernée un droit à l'information préalable à tout traitement de données médicales, fixent les conditions dans lesquelles le consentement de la personne concernée doit être requis et assurent à la personne concernée le respect de son droit d'accès. Deux autres recommandations régissant d'une part le traitement des données personnelles à des fins statistiques et d'autre part le traitement de données personnelles à des fins d'assurance privée sont en cours d'élaboration. En ce qui concerne cette dernière, nous avons assisté à une deuxième réunion du groupe de travail 14 à Strasbourg. La question du contenu de la clause de consentement y a notamment été abordée, ainsi que celle de l'opportunité d'assimiler les données financières à des données sensibles.

Pour sa part, le Comité consultatif mis en place par la Convention 108 et qui est chargé en particulier de donner des avis sur l'application de ladite Convention s'est penché plus particulièrement sur la définition de données à caractère personnel. Il a en particulier admis que la voix et l'image, lorsqu'elles permettent d'identifier une personne, sont incluses dans cette définition. Le Comité n'a par contre pas encore définitivement tranché la question de savoir si le traitement de la voix et de l'image tombait dans le champ d'application de la protection des données. Cela devrait pour le moins être le cas lorsque la voix et l'image sont enregistrées sur un support automatisé permettant le traitement de l'information. Enfin, le comité consultatif a dû constater que l'utilisation du "contrat-type" pour les flux transfrontières élaboré en coopération avec l'Union européenne et la Chambre de commerce internationale n'avait pas eu l'écho escompté. Pour notre part, nous avons à plusieurs reprises conseillé à des entreprises ayant des activités transfrontières de conclure des contrats de protection des données basés sur ce modèle.

3. Organisation de coopération et développement économique (OCDE) - autoroutes de l'information et multimédias interactifs

Depuis l'adoption des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données, le 23 septembre 1980, l'OCDE tient régulièrement des réunions ad'hoc d'experts chargés de faire le point sur le suivi donné à ces directives et d'aborder des thèmes soulevant des problèmes spécifiques du point de vue de la protection des données. Une telle réunion a eu lieu à Paris du 30 novembre au 2 décembre 1994. Elle était consacrée aux infrastructures de l'information, en particulier les autoroutes de l'information et les multimédias interactifs. Par le biais d'exemples concrets, nous avons pu mesurer, outre les avantages offerts par les nouvelles technologies, les risques d'atteinte au droit de la personnalité générés par ces moyens. Ont ainsi été mis en évidence certains aspects pervers et cachés de ces technologies qui, sous prétexte de permettre à des clients potentiels de faire à la maison leurs achats de consommation courante ou même vestimentaire au moyen de leur PC ou de leur télévision interactive, enregistrent en même temps à des fins de ciblage de l'offre toutes les interventions de la personne concernée dans le système informatique. Ainsi, il sera possible de tirer, à partir des interactions faites par le client lui-même, d'innombrables informations sur ses habitudes, ses demandes ou attentes et ensuite, à l'insu de cette personne, d'adapter les offres de produits ou même d'influencer ses comportements d'achat. De la sorte, des profils de la personnalité pourront être constitués.
Il a également été relevé que les styles de vie, les régimes de travail et les transactions commerciales seront transformés au fur et à mesure de l'introduction de l'informatique et des réseaux dans chaque domicile et entreprise. Ces réseaux relieront en effet les administrations publiques, les foyers, les entreprises publiques et autres organismes, à une gamme très étendue de services interactifs tels que services sociaux ou administratifs, loisirs, formation, culture, banques de données, opérations financières de paiement, opérations bancaires, démarchage publicitaire ou commerce électronique. Cette évolution ne doit cependant pas se faire au détriment des droits de la personnalité des individus. Avec les autres participants à cette réunion, nous avons dressé un inventaire illustratif des risques répertoriés et des atteintes concrètes déjà constatées lors des premières expériences d'utilisation d'autoroutes de l'information dans différents pays: collectes abusives de données

personnelles, intrusions indésirables à la suite d'achats par téléréseaux, échanges entre autorités publiques d'informations personnelles réutilisées à d'autres fins que celles indiquées lors de la collecte, procédés abusifs utilisés par certains "télévendeurs", courrier publicitaire ciblé, élaboration de profils de la personnalité constitués sur la base des interactions des personnes dans le multimédia, ou encore surveillance des styles et modes de vie des utilisateurs de ces technologies.
Un débat s'en est suivi sur les démarches à entreprendre face à ce phénomène. Il a été à cette occasion relevé que ces nouvelles technologies font partie intégrante de notre société moderne et qu'il convient non pas de les combattre, mais au contraire d'en étudier les mécanismes et de mettre en place des stratégies permettant leur développement dans le respect des droits de la personnalité des individus. En tant que point fort de ces stratégies, outre l'élaboration de lois ou de réglementations, de codes ou de normes volontaires ou même de solutions techniques ou organisationnelles, les participants ont convenu que de gros efforts devront être entrepris dans "l'éducation" ou la "sensibilisation" des individus à ces dangers. Chaque personne sera ainsi en mesure d'agir en connaissance de cause dans ce nouvel environnement informatique. Notre politique d'information, établie comme l'une de nos priorités, se place dans cette perspective.
Certaines expériences menées notamment au Canada démontrent d'ailleurs que la transparence contribue non seulement à améliorer la protection des données, mais sert également les intérêts économiques. Les experts ont en outre souligné l'importance de technologies, telles les mesures "cryptographiques", permettant des transactions anonymes. Ils ont finalement mis en évidence le rôle complémentaire des mesures de sécurité, en tant que moyens permettant de garantir la protection des données et le respect de la vie privée.

4. Union européenne

Comme nous l'avions signalé dans notre premier rapport (p. 157), la commission européenne a présenté en octobre 1992 une deuxième mouture du projet de directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qu'elle a transmise au Conseil des Ministres. Ce second projet a fait l'objet de discussions approfondies parmi les experts gouvernementaux qui l'ont passablement amendé. Le projet a été adopté par le Conseil des Ministres, le 20 février 1995 et transmis au Parlement. La directive pourrait ainsi entrer en vigueur au début de l'année prochaine. Quant au projet de directive concernant la protection des données à caractère personnel et de la vie privée dans le contexte des réseaux de télécommunications numériques publics, en particulier du réseau numérique à intégration de services (RNIS) et des réseaux numériques mobiles publics, il a été finalisé par la commission et pourrait être adopté cette année encore. Une fois ces projets formellement adoptés, il conviendra d'en étudier les implications pour la Suisse, notamment sous l'angle des flux transfrontières de données. D'autres travaux sont également en cours dans des domaines particuliers, notamment dans le secteur douanier.

5. Schengen

Signée par neuf Etats membres de l'Union européenne (France, Allemagne, Belgique, Luxembourg, Pays-Bas, Espagne, Portugal, Italie, Grèce), la Convention

de Schengen est entrée en vigueur le 26 mars de cette année entre sept Etats. L'Italie et la Grèce ne remplissent pas encore toutes les conditions juridiques et techniques, notamment celles liées à la protection des données, nécessaires à la mise en oeuvre de la Convention. Cette Convention qui permet la suppression des contrôles frontières dans les Etats de la sphère Schengen, règle en particulier la circulation des personnes et la coopération policière, douanière et judiciaire. Elle met en place un vaste système d'information Schengen (SIS) assisté par ordinateur qui doit permettre un échange rapide d'informations et un accès rapide aux fichiers de recherches informatisés concernant les personnes, les véhicules et les objets. Le SIS est composé d'une partie centrale qui assure la fonction de support technique du système et d'une partie nationale dans chaque Etat membre. Afin d'assurer la protection des données, la Convention contient des règles détaillées qui s'appuient sur la Convention 108 et sur la Recommandation du Conseil de l'Europe n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Cette recommandation fait d'ailleurs partie intégrante de la Convention Schengen. La Suisse n'est pas membre de Schengen et ne peut pas à l'heure actuelle le devenir, n'étant pas membre de l'Union européenne. Cependant notre pays a tout intérêt à se rapprocher de ces Etats, notamment dans le cadre de la lutte contre la criminalité organisée, le trafic de drogue ou le contrôle de l'immigration. Nous sommes d'avis que ce rapprochement doit se faire dans le respect des dispositions nationales de la protection des données et être encadré de règles identiques à celles prévues dans la convention Schengen. En ce sens, une coopération institutionnalisée a notre préférence et devrait être privilégiée.

IV. REGISTRE DES FICHIERS

1. Bilan

Le seuil des 1'500 déclarations de fichiers évoqué dans notre premier rapport a été atteint et sera prochainement dépassé, quelques offices ne nous ayant pas encore fait parvenir leurs annonces. Malgré les difficultés que nous rencontrons, notamment par manque de ressources humaines, tant du côté des conseillers à la protection des données que du nôtre, DATAREG et le registre des fichiers sont en passe de devenir à moyen terme un "outil" performant.

Les difficultés signalées dans notre premier rapport sont encore d'actualité, en particulier au sein de l'administration fédérale, quelques offices n'ayant pas encore annoncé leurs fichiers ou ne l'ayant fait qu'incomplètement. Nous ne disposons d'autre part pas des ressources humaines suffisantes pour être en mesure de procéder efficacement au contrôle des formulaires de déclaration et publier le registre des fichiers dans la forme et les délais prévus. En outre, il est rare que les conseillers à la protection des données nommés par les départements et par certains offices soient en mesure de nous seconder dans notre tâche, notamment en organisant la procédure d'annonce et les traductions, vu qu'en règle générale ni le temps, ni les moyens nécessaires ne leur ont été accordés par les unités administratives dont ils relèvent.
Dans le secteur privé, des annonces nous sont parvenues des branches les plus diverses, tels le secteur automobile, les banques, le commerce de détail, les re-

gistres des tumeurs, les églises, la télématique, la presse etc. Les contacts établis dans le cadre de la procédure de déclaration nous sont non seulement utiles pour l'élaboration du registre des fichiers, mais ils nous permettent également de nous familiariser avec les modalités de fonctionnement de ces secteurs, et surtout d'informer, respectivement sensibiliser les maîtres de fichiers privés à la protection des données.
Finalement, malgré les contretemps susmentionnés, DATAREG, respectivement le registre des fichiers, prennent forme, guérissant peu à peu de leurs "maladies d'enfance" pour devenir à moyen terme à la fois "la clé du droit d'accès pour les personnes concernées" et un instrument de travail performant pour nous.

2. DATAREG - Système de gestion du registre des fichiers

Suite à l'entrée en fonction, en juiller 1994, du système automatisé pour la gestion des données du registre des fichiers (DATAREG), nous disposons maintenant des premières exploitations des fichiers déjà saisis.

DATAREG est entré officiellement en activité chez nous le 4 juillet 1994. Le 16 juin 1994, 462 déclarations de fichiers d'organes fédéraux sont arrivées, dont 16 étaient prêtes à être enregistrées et introduites dans DATAREG. 94 fichiers ont été annoncés par des personnes privées dont 10 étaient prêts à l'introduction dans DATAREG. Une déclaration est prête à l'introduction dans DATAREG lorsqu'elle a passé l'examen sommaire de son caractère licite, tel qu'il est prévu par la loi, et qu'elle est présentée en trois langues (allemand, français et italien). Jusqu'à la fin janvier 1995, 1'500 déclarations sont arrivées auprès du PFPD, dont 200 émanent de personnes privées.

La situation en janvier 1995 fait état des réalisations suivantes:

- A cette période, 111 fichiers au total sont enregistrés, dont 104 proviennent d'organes fédéraux. De ces 111 fichiers enregistrés, tous doivent être publiés, à l'exception de deux. Toutes les saisies doivent être effectuées en trois langues. Selon les indications sur les déclarations de fichiers, 102 *adresses* (p. ex. maîtres du fichier, personne habilitée à renseigner, etc.) ont été enregistrées dans le système jusqu'à ce jour.
- Sur les formules de déclaration, 17 catégories de données personnelles traitées figurent à choix et à titre d'exemples. Toutefois 188 catégories différentes de données personnelles ont été mentionnées sur les déclarations déposées. Ces catégories sont utilisées 530 fois en tout, ce qui signifie que, par déclaration, en moyenne cinq catégories de données personnelles exploitées ont été désignées.
- 143 catégories de destinataires de données ont été enregistrées dont 41 figurent aussi comme participants. On peut en déduire qu'en moyenne un fichier enregistré sur deux possède une catégorie de participants, et qu'en règle générale une catégorie de destinataires au moins est attribuée à chaque fichier enregistré. Des données de ces fichiers sont par conséquent communiquées à des tiers.
- En ce qui concerne les déclarations faites par les organes fédéraux, 56 bases juridiques différentes ont été citées jusqu'à présent. Ces dernières ont été

appliquées 154 fois. Cela signifie qu'en moyenne plus d'une base légale (loi/ordonnance) pour l'exploitation du fichier est annoncée par déclaration.
- Quatre catégories de branches ont été attribuées pour la saisie de fichiers privés.
- Après l'enregistrement dans DATAREG, l'organe qui procède à la déclaration reçoit un imprimé de contrôle avec le numéro d'enregistrement du fichier et les données qui ont été saisies dans DATAREG.

Différentes corrections et adaptations ont été apportées au système DATAREG. Celles-ci ont été rendues nécessaires, d'une part du fait qu'il s'agit d'une nouvelle procédure d'annonce, d'autre part en raison de nécessités d'ordre technique. Ainsi par exemple, il a fallu adapter les dimensions des champs et les désignations masculines et féminines sur les extraits de registre imprimés et adressés pour vérification aux maîtres de fichiers concernés.

V. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

1. Evolution des tâches

Cette année également, le volume des tâches a augmenté dans presque tous les domaines. Les questions relatives aux conditions de déclaration des fichiers ont été particulièrement abondantes. De même, nous avons reçu de nombreuses demandes concernant le droit d'accès, les violations de la personnalité et les éventuels motifs justificatifs, les communications de données à l'étranger, l'applicabilité des dispositions cantonales et bien d'autres encore.

2. Information du public

Durant tout l'exercice, nous avons participé à diverses manifestations (conférences, rencontres) concernant la protection des données. Notre présence a permis de familiariser divers milieux avec le droit de la protection des données et l'opportunité de son application, et de résoudre à cette occasion un certain nombre de problèmes.

Cette année, nous avons adressé au total 5000 brochures, dans l'une ou l'autre des trois langues officielles, à des autorités ainsi qu'à des personnes privées. Une nouvelle brochure sur la protection des données dans les rapports de travail privés est venue s'ajouter aux quatre précédentes publications.

Les brochures suivantes sont disponibles auprès du PFPD:

- Guide pour le traitement des données personnelles dans l'administration fédérale
- Guide à l'usage des maîtres de fichiers (domaine privé)
- Les droits de la personne concernée en matière de traitement de données personnelles
- Guide relatif aux mesures techniques et organisationelles de la protection des données
- Guide pour le traitement des données personnelles dans le secteur du travail (domaine privé).

Nous avons finalement saisi à deux reprises l'occasion d'informer le public par communiqué de presse, au sujet de la problématique des formulaires d'inscription pour les candidats à la location d'un logement (cf. p. 154 ss) et de la consultation de données relatives aux détenteurs de véhicules par le biais du numéro 111 (cf. p. 169 ss).

Service téléphonique du PFPD

Au cours de cette année, nous n'avons pas seulement répondu à des questions par la voie de la correspondance officielle. Nous avons également fourni de nombreux renseignements par téléphone.

Le tableau qui suit en page 189 donne un aperçu des domaines dans lesquels nous avons fréquemment été consultés.

L'annonce de fichiers, les communications de données à l'étranger et l'exercice du droit d'accès sont les domaines qui ont suscité le plus vif intérêt. Les questions émanant du secteur privé (particuliers, milieux professionnels et de l'industrie, associations, avocats etc.), au total 870 appels, étaient plus nombreuses que celles provenant des organes fédéraux, totalisant 230 appels.

3. Dotation en personnel du secrétariat du PFPD

Bien que le personnel du Secrétariat ait légèrement augmenté au cours de l'exercice écoulé, il nous est impossible d'accomplir toutes nos tâches d'une manière satisfaisante. Il est prévu à ce propos d'engager des collaborateurs supplémentaires. Cet accroissement du personnel nous permettra d'entamer les travaux nécessaires dans le domaine de la levée du secret médical. De nombreux autres domaines d'activités devront néanmoins demeurer en attente.

4. Formation et perfectionnement

En raison de la rapide évolution de la protection des données, tant du point de vue juridique que technique, nos collaborateurs et collaboratrices ont de plus en plus besoin de bénéficier d'une formation supplémentaire. Il est particulièrement important de suivre l'évolution au niveau international pour que nous soyons en mesure de trouver pour notre sphère d'activités des solutions adaptées aux circonstances actuelles. Pour l'instant, dans maintes situations, les moyens et le temps de suivre les cours nécessaires font défaut.

5. Statistique des activités du Préposé fédéral à la protection des données Période du 1er avril 1994 au 31 mars 1995

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

Préposé fédéral à la protection des données :	Guntern Odilo, dr en droit
Suppléant :	Walter Jean-Philippe, dr en droit
Secrétariat :	
Chef:	Walter Jean-Philippe, dr en droit
Suppléant:	Buntschu Marc, lic. en droit
Service juridique :	7 personnes
Service informatique :	3 personnes
Service de l'information :	Tsiraktsopulos Kosmas, lic. en droit
Chancellerie :	3 personnes

VI. RECOMMADATIONS DU PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES