Préposé fédéral à la protection des données

Rapport d'activités 1993/94

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 juillet 1993 au 31 mars 1994.

TABLES DE MATIERES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

REPERTOIRE DES ABREVIATIONS

ADN	Acide désoxyribonucléique
AFIS	Système automatique d'identification des empreintes digitales AFIS: Automatic Fingerprints Identification System
ASBCEF	Association pour la gestion d'un centre d'informations de crédit
ASTERIX	Index automatisé du casier judiciaire
AUDIT	Procédure de contrôle
AUPER	Système d'enregistrement automatisé des personnes
AVS	Assurance vieillesse et survivants
CI 95	Carte d'identité
CJ-PD	Groupe de projets sur la protection des données
CO	Code des obligations
CP	Code pénal
cst	Constitution fédérale
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DOSIS	(Projet-pilote) Système provisoire de traitement des données en matière de drogue
FF	Feuille Fédérale
FMH	Fédération des Médecins Suisses FMH: Foederatio Medicorum Helveticorum
ISIS	Système provisoire de traitement des données relatives à la protection de l'Etat
JAAC	Jurisprudence des autorités administratives de la Confédération
LPD	Loi fédérale sur la protection des données
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
LSEE	Loi fédérale sur le séjour et l'établissement des étrangers
LSF	Loi sur la statistique fédérale
MOFIS	Système informatisé de véhicules à moteur
OCDE	Organisation de coopération et de développement économique
OFCOM	Office fédéral de la communication
OFI	Office fédéral de l'informatique
OFPER	Office fédéral du personnel
OK	Système de traitement des données pour l'exploitation d'informations utiles à la lutte contre le crime organisé
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
PERIBU	Système de gestion informatisé du personnel
PFPD	Préposé fédéral à la protection des données
PIAS	Système de gestion et administration du personnel
PISA	Système de gestion du personnel de l'armée
PISEDI	Système de gestion du personnel du DFI
RCE	Registre central des étrangers
REE	Registre des entreprises et établissements
REGI	Gestion informatisée des personnes et des dossiers
RIPOL	Système de recherches informatisées de police
RNIS	Réseau numérique à intégration de services
RS	Recueil Systématique
SET	Système de calcul électronique du temps de travail
SIDA	Syndrome immuno-déficitaire acquis

SPO	Organisation suisse des patients
SUPIS	Système de gestion informatisé du personnel Sulzer
TED	Traitement électronique de données
VIH	Virus de l'immunodéficience humaine
ZAN	Index central des dossiers du bureau central suisse de police
ZEK	Centre d'informations de crédit

PREFACE

La loi fédérale du 19 juin 1992 sur la protection des données (LPD) et les ordonnances d'exécution qui s'y rapportent sont entrées en vigueur le 1er juillet 1993. Ceci a permis de combler une importante lacune dans notre ordre juridique. La nouvelle loi définit un nombre de principes de traitement des données qui doivent être respectés par tous les maîtres de fichiers qui sont soumis à la loi.
La protection des données ne peut cependant pas être assurée qu'avec des principes matériels, la loi n'étant pas en mesure d'apporter une réponse au large éventail de problèmes de protection des données actuels. Pour que la protection des données soit vraiment appliquée, il est impératif que la société prenne conscience de la nécessité d'une telle protection. La meilleure protection de la sphère privée est un public bien informé qui - en connaissance de cause des problèmes existants dans ce domaine - est en mesure de défendre ses droits dans son propre intérêt.

Le premier rapport d'activité du Préposé fédéral à la protection des données (PFPD) s'efforce entre autre de contribuer à cette prise de conscience en informant le public des tâches accomplies par le Secrétariat du PFPD durant la première année de son activité.
Ce premier rapport décrit la situation actuelle au niveau de la protection des données dans le secteur privé ainsi que dans l'administration fédérale en Suisse. Dans le but de respecter le libre choix des citoyennes et citoyens quant à l'information, nous rapporterons aussi bien des faits positifs que négatifs. Dans notre société moderne et complexe, le droit des citoyennes et citoyens à la protection de leur sphère privée est constamment mis en danger.
Bien que nous ayons contribué à résoudre divers problèmes, il n'est pas exclu qu'à l'avenir, de nouvelles difficultés surgissent en matière de traitement de données personnelles. De même y aura-t-il toujours des voix qui s'élèveront pour exiger moins de protection des données et plus de pouvoir d'intervention en faveur de l'Etat. Pourtant, le recours croissant à l'automatisation du traitement des données personnelles et les interconnexions entre systèmes TED ne constituent pas la seule solution à tous les problèmes de notre société. Le traitement inconsidéré de données personnelles contient en soi des risques dont les conséquences sur notre environnement social ne doivent pas être sousestimés.

La protection des données contribue de manière déterminante à protéger la sphère privée des citoyennes et citoyens. Nous sommes cependant conscients du fait qu'une protection intégrale de la personnalité n'est pas réalisable dans une société moderne. Nous nous engagerons cependant toujours pour que chaque individu conserve un droit de codécision quant aux droits en faveur desquels sa sphère privée pourra être restreinte. En effet, le droit de la personne concernée à l'autodétermination en matière d'information doit être garanti de manière aussi complète que possible. Ce droit doit, à l'instar du droit à la protection de la personnalité, être respecté tant par les citoyennes et citoyens que par les autorités. La protection des données est dans l'intérêt de tous ceux qui sont concernés par des traitements de données, et il est réjouissant de constater que le public et l'administration dans leur majorité sont prêts à garantir ce droit.

Un débat animé a lieu actuellement sur des sujets tels que la sécurité intérieure, l'écoute de conversations téléphoniques, la nouvelle carte d'identité, la recherche dans le domaine du génie génétique, pour ne citer que quelques exemples. Il s'agit là

de domaines dans lesquels la protection des données personnelles est une nécessité. Nous suivrons de près leur évolution et tenterons, en collaboration avec les organes compétents, de résoudre les problèmes de protection des données qui se posent.

I. THEMES CHOISIS

1. Affaires de police

1.1. "1994, sûreté intérieure"; en tenant compte de la protection des données?

Le phénomène général de multiplication des traitements de données au sein de notre société lié aux développements technologiques a provoqué un accroissement inquiétant des risques d'atteinte à la personnalité des individus. Ce phénomène est particulièrement criant dans le domaine spécifique de la police.

Bien que cette évolution se soit déjà amorcée depuis maintenant quelques années, la période 1993-1994 a connu un véritable coup d'accélérateur en ce qui concerne ce que l'on peut appeler le développement des "nouveaux moyens" de police. On peut ainsi citer non seulement la mise en place effective de nouveaux systèmes informatisés de police tel que le système provisoire de traitement des données relatives à la protection de l'Etat [ISIS] mais également le développement de toute une série de projets informatiques afférents à différentes autorités policières tels le système provisoire de traitement des données en matière de drogue [projet-pilote DOSIS], la banque de données sur le crime organisé [OK] ou encore la banque de données centrale relative à la nouvelle carte d'identité [CI 95].

Cette tendance à l'accroissement des moyens de police ne touche pas uniquement la création de nouveaux systèmes mais aussi la mise en place de *liaisons en ligne (online) toujours plus nombreuses* permettant aux autorités d'accéder directement à différents systèmes. Nous pouvons mentionner à titre d'exemples le système de recherches informatisées de police [RIPOL], le registre central des étrangers [RCE/ZAR], le système d'enregistrement automatisé des personnes [AUPER], l'index automatisé du casier judiciaire [ASTERIX], le système informatisé de véhicules [MOFIS], l'index central des dossiers du bureau central suisse de police [ZAN] ou encore le nouveau système provisoire de traitement des données relatives à la protection de l'Etat [ISIS]. A ce sujet, nous vous conseillons de vous reporter à la partie de ce rapport consacrée aux "nouveaux dangers" et au "schéma" illustrant cette inflation de liaisons.

Ces systèmes sont en outre parfois *interconnectés*. Voici à titre d'exemples l'index central des dossiers [ZAN], relié au système automatique d'identification des empreintes digitales [AFIS], aux informations du service INTERPOL et au futur système provisoire de traitement des données en matière de drogue [projet-pilote DOSIS], ainsi que le registre central des étrangers [RCE], connecté au système d'enregistrement automatisé des personnes [AUPER] et au registre des entreprises et établissements [REE].

Il convient enfin de relever que parallèlement à cette expansion de moyens technologiques de police, sont élaborés de *nouveaux textes législatifs*. Ces derniers ne servent pas seulement de réglementations pour les systèmes informatisés de police. Ils visent également à créer les bases légales relatives à la sécurité intérieure, à la lutte contre la criminalité ou à la mise sur pied des services centraux et des agents de liaison. L'élaboration de ces normes a permis de mettre en évidence la difficulté toujours plus grande de concilier les intérêts des autorités de police avec les

principes de la protection des données. Ainsi, la remise en cause systématique de l'exercice du droit d'accès en matière de lutte contre le crime organisé et de sécurité intérieure - alors que ce droit est garanti dans la loi sur la protection des données - illustre parfaitement cette problématique.

Les exemples susmentionnés soulignent à quel point les développements technologiques dans le domaine policier vont de pair avec l'augmentation des *risques d'atteintes aux droits fondamentaux* et à la personnalité des citoyennes et des citoyens. Ces risques sont encore accrus par l'élaboration de normes juridiques permettant de justifier des restrictions aux droits des individus toujours plus importantes. Dans le cadre d'un programme d'action spécial, le Département fédéral de justice et police a décrété 1994 "année de la sûreté intérieure" . Il conviendra dans ce contexte de veiller à ce que ce plan d'action ne soit pas réalisé au détriment de la protection des données.

1.2. Protection des données de police: les nouveaux dangers!

Nous avons rappelé à plusieurs reprises que, contrairement à une fausse idée largement répandue, la protection des données ne vise pas à protéger les criminels au détriment de l'efficacité des activités de police. Elle a pour but de mettre en place un cadre légal précis, réglant les conditions dans lesquelles des traitements de données doivent être effectués. Ce cadre légal doit concilier les intérêts des autorités de police à accomplir leurs tâches et le respect des droits fondamentaux et de la personnalité des personnes concernées. Nous avons également souligné que cette pondération des intérêts en présence doit être effectuée de manière toujours plus pointue, les développements technologiques dans le domaine policier et la mise en évidence d'une série de "nouveaux dangers" allant de pair avec une augmentation des risques d'atteintes aux droits de la personnalité des individus. Ces "nouveaux dangers" concernent notamment l'extension constante des systèmes de police existants, la création infondée de bases légales permettant de tout justifier ou encore la mise en place d'un nombre toujours plus impressionnant de liaisons en ligne (online) habilitant de nombreuses autorités différentes à accéder directement aux banques de données de police. Nous avons finalement constaté qu'il devient toujours plus difficile pour un citoyen ou une citoyenne d'appréhender les véritables enjeux et dangers inhérents à la création de nouveaux systèmes informatisés de police.

Création de bases légales pouvant tout justifier et inflation dangereuse des liaisons en ligne (online): l'exemple de la représentation schématisée de certains systèmes informatisés de police

La loi fédérale sur la protection des données prévoit que les organes fédéraux ne sont en droit de traiter des données personnelles que s'il existe une base légale à cet effet. Elle stipule en outre qu'un organe fédéral n'est en droit de rendre des données personnelles accessibles au moyen d'une procédure d'appel (online) que si cela est prévu expressément; de plus, cette exigence doit être remplie au niveau d'une loi au sens formel lorsque la liaison en ligne permet l'accès à des données sensibles ou à des profils de la personnalité.

Nous avons été amenés à de nombreuses reprises à rappeler que ces exigences doivent être respectées pour tout traitement de données personnelles. Mais nous avons également dû faire face à la nouvelle tendance de certains organes à vouloir justifier tout traitement de données par la seule création de bases légales. A cette

tendance vient en plus s'ajouter la soif de nombreuses autorités d'accéder à un nombre croissant de systèmes informatiques, ce qui a notamment pour conséquence une augmentation du risque de détournement de la finalité de nombreux systèmes. Ceci est particulièrement dangereux dans le domaine spécifique de la police en raison de la sensibilité des données qui y sont traitées.

Dans ce contexte, nous avons attiré l'attention des organes fédéraux concernés sur le fait que le respect du principe de la légalité vise avant tout un but de transparence, et qu'il ne suffit pas à lui seul à légitimer un traitement de données personnelles. La mise en place d'une liaison en ligne (online) doit être précédée d'un examen de sa nécessité et de sa conformité aux principes de proportionnalité et de finalité. En d'autres termes, les traitements de données et les accès en ligne ne peuvent pas uniquement être prévus dans des bases légales, mais ils doivent également être conformes aux principes généraux de la loi sur la protection des données. Face à l'ampleur des nombreuses liaisons en ligne (online) et aux dangers qu'elles engendrent, nous devons donc veiller, lors de l'examen d'une demande d'accès en ligne à un système, à ce que la liaison prévue soit conforme aux principes généraux de la LPD, et ce avant que ne soit élaborée ou approuvée la base légale devant autoriser un tel accès.

Afin de permettre une approche plus explicite et visuelle de cette problématique, nous avons élaboré *un schéma* représentatif de quelques systèmes informatiques de police relativement "médiatiques", en fonction ou en voie d'élaboration. Ce schéma illustre l'ampleur des liaisons en ligne (online) existantes ou envisagées en faveur de nombreuses autorités. Il ne constitue qu'un extrait de l'ensemble des systèmes de l'administration fédérale. Cette précision a son importance puisqu'en dépit de son caractère impressionnant, ce schéma ne représente en fait qu'une goutte d'eau dans l'océan informatique fédéral.

Deux remarques

- Les liaisons en ligne (online) retranscrites sur ce schéma ne représentent pas toutes des accès à l'intégralité des données d'un système. De nombreuses liaisons ne permettent en fait l'accès qu'à une partie des données d'un système selon la matrice d'accès y relative.

- Ce schéma comprend certains systèmes non encore en fonction. Toutes les liaisons représentées sont toutefois, soit effectives ou autorisables en vertu de dispositions de lois ou d'ordonnances en vigueur, soit envisagées dans le cadre de projets législatifs publiés (Message du Conseil fédéral, procédure de consultation ouverte).

Les véritables enjeux et dangers inhérents à la création d'un nouveau système informatique de police: l'exemple de la nouvelle carte d'identité [CI 95]

Dans le cadre de son projet de mise en circulation d'une nouvelle carte d'identité suisse [CI 95], l'Office fédéral de la police a mis en consultation au début de l'année un projet d'ordonnance du Conseil fédéral. Cette ordonnance a pour but de réglementer non seulement la procédure d'émission de cette nouvelle carte d'identité, mais également de fixer de manière très précise les conditions de traitement des données personnelles collectées à cet effet. Consultés dans la phase d'élaboration de ce projet, nous avons rendu les concepteurs du projet attentifs aux exigences liées à la protection des données qu'il convenait d'ancrer dans l'ordonnance relative à la carte d'identité. C'est ainsi qu'ont été expressément déterminées les données qui pourront être collectées pour remplir la formule de demande, les données qui seront inscrites sur la carte, ainsi que celles qui seront enregistrées dans la banque de données centrale gérée à Berne par l'Office fédéral de la police. Nous avons également demandé que le "cheminement" de ces informations personnelles entre l'autorité d'établissement, le producteur de la carte et l'Office fédéral de la police soit clairement décrit. Le texte de l'ordonnance fixe au demeurant les différentes durées de conservation des données, à savoir sept jours auprès de la firme productrice, deux mois auprès de l'autorité d'établissement et quinze ans au maximum dans la banque de données centrale.

Lors de l'examen du concept CI 95, nous avons clairement insisté sur le fait qu'aucune donnée "cachée" ne doit être insérée dans la carte, ce qui implique que toutes les informations sont lisibles par son détenteur et partant, que cette carte ne doit contenir ni bande magnétique ni micro-chips. Ces exigences ont été respectées. Certes, le concept de l'Office fédéral de la police prévoit l'introduction sur la carte d'informations lisibles à la machine (MRIDs - Machine Readable Identification Documents) sous norme ICAO 9303 (International Civil Aviation Organization). Ce "code lisible par machine" a été introduit par les concepteurs du projet en tant qu'élément indispensable du concept de réalisation d'une telle carte d'identité. Mais ledit code est parfaitement lisible par le détenteur, ne consistant qu'en une retranscription des données déjà inscrites sur la carte. Lors de la procédure de consultation de l'ordonnance relative à la carte d'identité, de nombreuses confusions ont été faites par les personnes auxquelles ce projet était soumis pour la première fois. Ainsi, des craintes ont été formulées quant à l'utilisation de ce code lisible par machine. Le risque que ce code permette aux autorités de police ou aux douaniers d'accéder au système de recherches informatisées de police [RIPOL] ou au registre central des étrangers [RCE] a notamment été évoqué. Or il importe de préciser que, sur la base des informations techniques fournies par les concepteurs du projet, ce code lisible par machine n'a d'autre but que de faciliter le travail aux postes-frontières en permettant aux douaniers d'effectuer de manière beaucoup plus rapide leurs tâches de contrôle au moyen d'un appareil de lecture du code. Mais ce code lisible par machine n'attribue absolument aucun droit ou possibilité d'accès à l'une ou l'autre banque de données, vu qu'il ne constitue nullement une clef d'entrée à différents systèmes. Les accès au RIPOL ou au RCE sont réglementés légalement. Les autorités habilitées à accéder à ces systèmes le sont donc en vertu de normes légales et non pas par le biais de l'utilisation de la nouvelle carte d'identité.

Ces précisions ne changent par contre rien au fait qu'il convient d'être extrêmement prudent quant à l'utilisation de ce code lisible par machine. C'est pourquoi nous

avons exigé que l'utilisation de ce code soit clairement et restrictivement déterminée dans l'ordonnance, avec indication des autorités habilitées à en faire usage et mention de la liste exhaustive des cas d'utilisation légitime. Son emploi a ainsi été limité aux seules autorités compétentes en matière de contrôles aux frontières et ce uniquement à certaines fins spécifiques.

Les craintes exprimées ci-dessus vis-à-vis de ce code lisible par machine démontrent la difficulté d'appréhender les différents dangers liés à l'introduction de nouveaux moyens technologiques. En effet, si l'utilisation de ce code doit être surveillée et clairement réglementée, nous avons relevé un autre élément, moins "médiatique" mais nettement plus dangereux: pour gérer ces nouvelles cartes d'identité, une *banque de données centrale* à Berne va être mise en exploitation. Y seront enregistrées toutes les données d'identité, ainsi que la photo et la signature de toutes les personnes détentrices d'une nouvelle carte. En d'autres termes, tous les citoyens et citoyennes suisses détenteurs d'une carte d'identité seront enregistrés dans ce système informatique géré par l'Office fédéral de la police. Il est par conséquent absolument primordial que l'utilisation de cette banque de données soit strictement réglementée. Dans ce sens, nous avons demandé que l'ordonnance du Conseil fédéral stipule clairement que l'enregistrement des données dans le système informatique ne vise qu'à empêcher qu'une même personne se fasse délivrer plusieurs cartes et qu'à accélérer la procédure de renouvellement de la carte en cas de perte. Afin de garantir le respect du principe de finalité, nous avons également recommandé de préciser que l'Office fédéral de la police ne peut utiliser ces données que dans le cadre de l'exécution de cette ordonnance et non pour accomplir d'autres tâches légales de police. Dans la même optique, les différents services de l'Office fédéral de la police tels que les services centraux de lutte contre le trafic de drogue, le service RIPOL ou encore la section INTERPOL du bureau central suisse de police n'ont aucun droit d'accès à cette banque de données. C'est pourquoi il a été spécifié que seules y auront accès les personnes autorisées de la section de la police administrative de l'OFP chargée précisément des tâches de gestion des cartes d'identité et des passeports.

Cet exemple de la nouvelle carte d'identité démontre de manière très illustrative que le développement et l'utilisation de nouveaux moyens technologiques peuvent comporter, du point de vue des droits de la personnalité, un grand nombre de dangers, dont les plus importants ne sont pas toujours perceptibles de prime abord. Ainsi, les risques d'atteintes à la protection des droits fondamentaux des individus inhérents au fait de ficher de manière centralisée tous les citoyens et citoyennes suisses détenteurs d'une carte d'identité justifient largement les nombreuses exigences de protection des données que nous avons eu l'occasion de faire valoir dans le cadre de ce projet. Ces exigences ont été reprises avec succès dans le projet d'ordonnance élaboré par l'Office fédéral de la police. Nous devrons veiller non seulement à ce qu'elles soient strictement respectées, mais également à ce qu'elles ne soient pas amoindries par le biais, notamment, d'adaptations légales dues à de nouvelles demandes d'accès de certaines autorités.

1.3. Crime organisé

Création d'un office central de lutte contre le crime organisé

Nous avons émis un certain nombre de remarques relatives au Message du Conseil fédéral du 12 janvier 1994 concernant la modification du code pénal en vue de la création d'un office central de lutte contre le crime organisé. La plupart de ces remarques visant une meilleure prise en compte des exigences liées au respect des droits de la personnalité ont été prises en considération. Cependant, deux divergences de fond subsistent dans la version finale du projet. Il s'agit des restrictions à l'exercice du droit d'accès et de l'introduction d'une clause générale pour l'élaboration de futurs systèmes informatiques "d'autres offices centraux". L'examen de ces points dans le cadre des débats parlementaires permettra de prendre la mesure de la place laissée aux droits fondamentaux des citoyennes et des citoyens dans le cadre de l'élaboration de normes juridiques permettant de justifier des restrictions aux droits des individus toujours plus importantes.

Depuis l'année passée, le fort 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, s'est singulièrement intensifié.

Faisant suite au "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, un "second train de mesures" a été présenté par le biais du Message du Conseil fédéral du 30 juin 1993 sur la modification du code pénal et du code pénal militaire. Ce second train de mesures porte principalement sur le droit de communication du financier (article 305ter, 2e alinéa, CP) et sur la notion d'organisation criminelle (article 260ter CP). Dans cette même perspective, un nouveau message concernant la création d'un office central de lutte contre le crime organisé a été adopté par le Conseil fédéral le 12 janvier 1994.

Ce projet d'office central de lutte contre le crime organisé constitue en fait un ensemble de dispositions spéciales relatives aux traitements de données de police. Les différentes normes pénales proposées prévoient en effet non seulement que l'office central aura notamment pour tâche de traiter les informations montrant les connexions nationales et internationales d'organisations criminelles mais elles règlent également les compétences des agents de liaisons, l'obligation d'informer imposée à certaines autorités, les modalités de communication et de renseignements provenant d'autres services, la recherche et la collecte des informations, le traitement des données personnelles, la mise en place d'un système informatique pour l'exploitation d'informations utiles à la lutte contre le crime organisé, la communication de données personnelles ainsi que l'exercice du droit d'accès.

Dans le cadre de la procédure de consultation, ce projet a été distribué à plus d'une vingtaine d'offices concernés. Toutefois, bien qu'afférant directement à la protection des données, il ne nous a dans un premier temps pas été fourni. Ce n'est qu'après avoir été expressément demandés à l'Office fédéral de la police que les textes mis en consultation ainsi que le message y relatif nous ont été transmis pour prise de position. Nous avons émis dans notre avis de nombreuses réserves concernant principalement la collecte d'informations à l'insu des personnes concernées, l'accès

online au système informatique par les organes fédéraux chargés de la sécurité intérieure ainsi que les restrictions apportées au droit d'accès.

Il a été tenu compte de certaines de nos remarques, principalement par l'introduction d'un droit d'information a posteriori de la personne concernée ayant fait l'objet à son insu d'une collecte de données personnelles et par la limitation de l'accès online des autorités fédérales chargées du maintien de la sûreté intérieure uniquement aux données sommaires d'identification enregistrées dans la banque de données sur le crime organisé. Cependant, non seulement les vives réserves émises à propos des restrictions au droit d'accès n'ont pas été retenues mais plus grave, le projet remanié transmis au Conseil fédéral pour approbation a d'une part été complété avec une nouvelle disposition autorisant "d'autres services centraux" à gérer des systèmes de traitement de données et a d'autre part été présenté comme ayant notre accord. En vertu des dispositions de la loi fédérale sur la protection des données et de l'ordonnance y relative, nous avons alors adressé un rapport à l'attention du Conseil fédéral afin de rendre ce dernier attentif aux lacunes constatées au niveau de la procédure de consultation et aux divergences matérielles encore existantes dans ce dossier. Malgré les nombreux séances et échanges de propositions ayant suivi cette intervention, aucune solution de compromis n'a pu être trouvée avec les différents représentants du Département fédéral de justice et police.

En ce qui concerne l*e droit d'accès* en particulier, en dépit des possibilités déjà offertes par la LPD de refuser, restreindre ou différer l'octroi de ce droit, le DFJP a opté pour l'élaboration d'une nouvelle réglementation spéciale beaucoup plus restrictive. Ainsi la personne concernée souhaitant exercer son droit devra faire valoir un état de faits concret et invoquer un intérêt particulier à l'information; en outre, la restriction au droit d'accès pourra être effectuée sans indication des motifs. Si nous pouvons reconnaître, sous certaines conditions, la pertinence de cette possibilité de ne pas motiver une restriction du droit d'accès, nous ne pouvons approuver les autres conditions supplémentaires mises à l'exercice de ce droit. 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 qui 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. En renvoyant au droit pertinent en la matière, le projet garantit cependant que chaque demande devra être examinée en procédant à une pesée concrète des intérêts en présence et en tenant compte du principe de la proportionnalité. Mais c'est surtout la condition imposée à la personne concernée de se référer à un état de faits concret qui n'est 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'autoaccuser 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 par la police d'une surveillance abusive ou infondée.

La disposition permettant à "d'autres offices centraux" chargés de la lutte contre des infractions déterminées de gérer un système de traitement des données conformément aux nouvelles dispositions pénales sur le crime organisé a également fait l'objet de critiques de notre part. Outre son manque de précision, cette norme équivaut en fait à une clause générale pour toutes les futures banques de données

qui seront élaborées dans le cadre de la lutte contre des infractions qui ne sont actuellement pas définies et qui seront gérés par des offices centraux encore indéterminés. Eu égard à l'augmentation croissante des nouveaux systèmes informatiques de police et à la mise en place de liaisons toujours plus nombreuses permettant à différentes autorités d'y accéder, une telle clause générale est inacceptable et va à l'encontre des dispositions de la loi sur la protection des données. Chaque système, dont l'élaboration doit avoir été précédée d'un examen quant à son opportunité, sa finalité et sa proportionnalité, doit faire l'objet d'une base légale qui lui est propre. Ce principe est en outre encore renforcé par le fait que les Chambres fédérales ont introduit dans la LPD une disposition prévoyant que les différentes liaisons directes (online) permettant d'accéder à des données sensibles - tel est le cas des systèmes informatiques de police - devront être expressément prévues dans une loi au sens formel. L'argumentation défendue dans le Message et tendant à justifier cette clause générale en vue de la mise en place définitive de la banque de données DOSIS relative à la lutte contre le trafic international de stupéfiants n'est pas pertinente. Une norme légale formelle devra en tout état de cause de toute façon être élaborée de manière spécifique pour cette banque de données sur la drogue afin que ses liaisons online puissent être expressément mentionnées. Le projet-pilote DOSIS a d'ailleurs sur ce point toujours été très clair en prévoyant, pour sa phase définitive, une modification de l'article 29 de la loi fédérale sur les stupéfiants.

Le projet de modification du code pénal visant à la création d'un office central de lutte contre le crime organisé a été approuvé par le Conseil fédéral dans sa séance du 12 janvier 1994. Nous avons pu constater à la lecture du message publié que certaines de nos revendications avaient été concrétisées avec succès. Les deux divergences restantes concernant respectivement les restrictions au droit d'accès et l'introduction d'une clause générale relative à de futurs systèmes informatiques "d'autres offices centraux" n'ont quant à elles pas été mentionnées dans le Message du Conseil fédéral qui précise laconiquement que "l*a réglementation stricte proposée est conforme à la législation fédérale en vigueur sur la protection des données; elle a également été discutée avec le Préposé fédéral à la protection des données*". Nul doute qu'elles seront certainement à nouveaux débattues dans le cadre des travaux parlementaires. Il conviendra alors de voir quelle place sera donnée aux droits fondamentaux et de la personnalité des citoyennes et des citoyens face à l'élaboration de normes juridiques permettant de justifier de toujours plus importantes restrictions aux droits des individus.

Le projet-pilote DOSIS

DOSIS constitue un projet-pilote élaboré par les services compétents du Département fédéral de justice et police dans le cadre de la mise en place d'une banque de données centrale sur la drogue. Géré par l'office central pour la répression du trafic illicite des stupéfiants près l'Office fédéral de la police, ce système aura notamment pour fonction, par le biais d'un accès online, d'assurer la coopération avec les brigades des stupéfiants des autorités cantonales de police. Dans sa séance du 23 mars 1994, le Conseil fédéral a adopté l'ordonnance DOSIS. Cette ordonnance a été élaborée par l'Office fédéral de la police avec notre collaboration. Elle contient toutefois une disposition particulière relative au droit d'accès que nous avions pourtant, dans le cadre d'une consultation sur un projet de norme similaire, qualifiée de "non conforme" à la LPD. L'introduction d'une telle restriction générale du droit d'accès au

niveau d'une ordonnance viole les prescriptions légales de protection des données pourtant adoptées au niveau d'une loi au sens formel par le Parlement.

Considéré comme prioritaire, ce projet a été élaboré selon un concept de réalisation en trois phases. La 1ère phase, entamée officiellement le 15 janvier 1993 et dénommée "phase interne", a été limitée à un traitement interne à l'office central des stupéfiants de l'Office fédéral de la police sans liaison avec les cantons; la collaboration entre autorités fédérales et cantonales chargées de la lutte contre le trafic de drogue est assurée, encore actuellement, par des employés cantonaux se déplaçant à Berne. La 2ème phase dite "externe", prévoit la mise en place de liaisons online de certains cantons au système informatique. Quant à la 3ème phase, elle correspond à la mise en fonction de la banque de données définitive sur la drogue à laquelle seront reliés l'ensemble des cantons.

L'urgence de la mise en place d'une banque fédérale de données en matière de drogue et la nécessité d'ancrer cette dernière sur la base d'enseignements concrets ont conduit l'Office fédéral de la police à opter pour une réalisation en plusieurs étapes comprenant notamment une phase d'essai externe. Consultés dès le début des travaux d'élaboration de ce concept DOSIS, nous avons approuvé cette procédure d'élaboration en trois phases. Nous avons toutefois exigé que la 2e phase consistant en un essai externe ne permette le rattachement online que de 8 cantons clairement déterminés, qu'elle soit expressément limitée dans le temps, qu'elle ne soit mise en fonction qu'avec l'entrée en vigueur d'une ordonnance y relative et enfin qu'elle soit effectuée en application des dispositions de la loi fédérale sur la protection des données. Cette dernière condition implique notamment le respect de la réglementation relative au droit d'accès prévue dans la LPD. Quant à la 3ème phase, nous avons rappelé qu'en vertu de la LPD, elle nécessite la mise en place d'une base légale formelle prévoyant expressément le recours aux liaisons directes des brigades cantonales des stupéfiants. Il a alors été convenu qu'à l'expiration de la phase d'essai, une modification de l'article 29 de la loi fédérale sur les stupéfiants sera élaborée, permettant d'ancrer légalement la banque de données définitive et de prévoir les liaisons online des brigades cantonales des stupéfiants des corps de police de tous les cantons.

Les travaux d'élaboration du projet d'ordonnance DOSIS ont été effectués par l'Office fédéral de la police, avec notre collaboration. Cette ordonnance règle en outre les buts du système informatique DOSIS, ses sous-systèmes et les données qui y seront traitées, les utilisateurs du système et leurs accès, le traitement des données, la saisie et le contrôle de qualité des données, la communication des données, les durées de conservation des données et leur effacement ainsi que les mesures de sécurité.

En marge des travaux d'élaboration de l'ordonnance DOSIS, l'Office fédéral de la police nous a demandé de nous prononcer sur deux points soulevés par certains cantons intéressés à participer au projet.

Le premier de ces points concerne l'application de la loi fédérale sur la protection des données au système DOSIS. Cette question a pu être résolue sans équivoque: DOSIS est un système fédéral, géré par l'Office fédéral de la police en coopération avec les cantons. Dans le cadre de sa phase d'essai externe avec liaison online des cantons, l'office central pour la répression du trafic illicite des stupéfiants près l'Office

fédéral de la police sera amené à examiner les données introduites dans DOSIS afin de s'assurer de leur conformité aux buts du système, vérifier les données saisies provisoirement et confirmer leur enregistrement définitif dans le cadre d'un concept de contrôle des données. A ce titre, en tant que système fédéral, DOSIS est donc soumis à la loi fédérale sur la protection des données et partant, au contrôle du Préposé fédéral à la protection des données. Ce contrôle ne portera toutefois d'une part que sur le système DOSIS et non pas sur les dossiers de police des cantons et ne s'effectuera d'autre part que dans les limites des compétences que nous attribue la loi fédérale sur la protection des données. Le cadre juridique du système DOSIS, en particulier l'application de la LPD, a ainsi été clairement précisé pour l'ensemble des participants au projet. La décision ultérieure du canton de Zürich de se retirer de l'essai-pilote DOSIS a été prise pour des raisons d'ordre technique liées au projet et ne relève pas de problèmes de protection des données.

Le second point soulevé par certains cantons se rapporte au droit d'accès. Ces derniers ont en effet exprimé leur crainte face aux dispositions de la loi fédérale sur la protection des données garantissant l'exercice de ce droit et ont demandé que des mesures puissent être prises afin de l'exclure ou tout au moins de le restreindre. Cette tendance visant à limiter l'exercice du droit d'accès aux banques de données de police est de plus en plus forte. Elle a d'ailleurs été concrétisée dans le cadre du 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 qui précise ainsi: "*Quant au droit de consultation, la Conférence des chefs des départements cantonaux de justice et police a, dans son avis du 8 septembre 1993, exigé que des mesures soient prises pour empêcher que la poursuite pénale ne soit entravée par l'application aveugle du droit de la protection des données. La formulation de l'article 351quindecies code pénal tient compte de cette préoccupation*".

Pour notre part, dans le cadre des travaux d'élaboration de l'ordonnance DOSIS, nous avons rappelé que la LPD ne règle pas seulement l'exercice du droit d'accès mais qu'elle prévoit expressément également tout un mécanisme permettant de refuser, restreindre ou suspendre l'exercice de ce droit. Le parlement, en adoptant la LPD, avait clairement vu la nécessité de prévoir de telles exceptions, principalement dans le domaine particulier des activités de police. Ces dispositions visant à restreindre l'exercice du droit d'accès vont ainsi déjà au-devant des doléances des autorités de police. Le projet-pilote DOSIS dans sa phase d'essai externe fondée sur une ordonnance du Conseil fédéral est donc parfaitement réalisable dans le respect des normes relatives à l'exercice et aux restrictions du droit d'accès prévues dans la loi fédérale sur la protection des données.

Toutefois, en dépit des considérations susmentionnées, une disposition particulière relative au droit d'accès à été introduite dans l'ordonnance DOSIS adoptée par le Conseil fédéral dans sa séance du 23 mars 1994. Cette norme stipule que "*le droit de consulter les données de DOSIS est ajourné jusqu'à l'entrée en vigueur de la modification du code pénal suisse (création d'un office central de lutte contre le crime organisé), mais au plus tard jusqu'au 31 décembre 1995*". Consultés en décembre 1993 par l'Office fédéral de la police sur un projet de disposition similaire, nous nous étions pourtant clairement prononcés en qualifiant une telle norme de "*non conforme à la LPD*". Nous avons notamment rendu attentifs les concepteurs du projet DOSIS au fait qu'il ne leur était pas possible d'introduire une restriction générale du droit d'accès au niveau d'une ordonnance. A cette occasion, il a été rappelé qu'en l'état

actuel de la législation et de la jurisprudence du Tribunal fédéral, les autorités de police peuvent refuser, restreindre ou différer la communication des renseignements demandés, soit dans la mesure où une loi au sens formel le prévoit ou des intérêts de tiers l'exigent, soit en raison d'un intérêt public prépondérant ou du risque de compromettre une procédure d'instruction et cela après avoir cas par cas procédé à une pesée concrète des intérêts en présence, dans le respect du principe de proportionnalité (article 9, 2e alinéa, LPD; ATF 113 Ia 268).

L'Office fédéral de la police a maintenu l'introduction de cette disposition d'exception pour DOSIS en se fondant sur l'article 9, 1er alinéa, lettre a LPD qui stipule pourtant explicitement la possibilité de restreindre le droit d'accès dans la mesure où une loi au sens formel le prévoit. Cet article de la LPD avait été adopté par les Chambres fédérales pour précisément éviter que des atteintes importantes aux droits fondamentaux des individus ne puissent être entérinées sans l'aval du Parlement. L'introduction d'une telle restriction générale du droit d'accès au niveau d'une simple ordonnance du Conseil fédéral n'est donc manifestement *pas conforme* à la LPD. Elle *viole* les prescriptions légales de protection des données pourtant adoptées au niveau d'une loi au sens formel par le Parlement!

Il conviendra dans ce contexte de tenir compte des résultats de l'examen par le Parlement du Message du Conseil fédéral relatif à la création d'un office central de lutte contre le crime organisé qui prévoit, mais cette fois au niveau d'une loi fédérale (en l'occurrence le code pénal), l'adoption d'une nouvelle norme restrictive quant au droit d'accès en matière de crime organisé (cf. commentaire dans le chapitre consacré à la création d'un office central de lutte contre le crime organisé). Ce projet entend également régler l'exploitation définitive de la banque de données sur la drogue DOSIS par l'adoption d'une norme consacrée aux futurs systèmes informatisés "d'autres services centraux". Dans ce contexte, devra alors être étudiée quelle révision devrait encore être apportée à l'article 29 de la loi fédérale sur les stupéfiants tel que cela avait été confirmé dans la réponse du Conseil fédéral à la question ordinaire Rechtsteiner du 28 avril 1993 concernant précisément le projet-pilote DOSIS.

1.4. Sûreté intérieure

Le système ISIS et le projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure

ISIS est le système informatique du Ministère public de la Confédération destiné à traiter les données relatives à la protection de l'Etat. Conçu en tant que système provisoire, il est actuellement en voie de réalisation. D'un point de vue juridique, les exigences de la protection des données ont été ancrées de manière détaillée dans une ordonnance du Conseil fédéral. A l'échéance de cette phase provisoire, les dispositions de l'ordonnance, en particulier celles relatives à l'effacement et aux durées de conservation des données, devront être réévaluées en tenant compte également des résultats des débats parlementaires portant sur l'examen du projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure adopté par le Conseil fédéral le 14 mars 1994.

ISIS est le système informatique provisoire de traitement des données relatives à la protection de l'Etat. Pour précision, il convient de relever que la nouvelle terminologie

en la matière fait référence "au maintien de la sûreté intérieure". Géré par le Ministère public de la Confédération, ce système est destiné à faciliter l'exécution d'enquêtes de police judiciaire dans les cas relevant de la juridiction fédérale et la mise en oeuvre de mesures préventives dans le domaine de la protection fédérale de l'Etat aux fins notamment de prévenir et combattre le terrorisme, le service de renseignements prohibé et l'extrémisme violent. Il est composé de cinq banques de données (protection de l'Etat, procédures pénales n'intéressant pas la protection de l'Etat, administration, documentation, système numérique). Ce système est actuellement en voie de réalisation. Depuis le mois de décembre 1993, deux sous-systèmes ont été mis en exploitation, à savoir les banques de données "administration" et "documentation". Les autres sous-systèmes devraient entrer en fonction dans le courant de l'année 1994.

Dans le cadre de la mise en place du système ISIS, les exigences de la protection des données ont été défendues avant tout sur un plan juridique. C'est ainsi qu'une ordonnance détaillée du Conseil fédéral a été élaborée dans le but de déterminer clairement quelles sont les finalités du système, quelles données pourront y être traitées, quels en sont les utilisateurs et à quelles donnnées ils sont habilités à accéder. Cette ordonnance règle également la saisie des données et leur contrôle de qualité, la communication des données, le mécanisme d'appréciation périodique des données, leur effacement ainsi que leur durée de conservation, l'exercice du droit d'accès des individus, les mesures de sécurité et les différents contrôles d'utilisation du système. N'ayant pas en mains de concept informatique détaillé quant à la réalisation technique du système actuellement en cours, nous avons rappelé au Ministère public de la Confédération que l'exploitation d'ISIS devrait se faire en parfaite conformité avec l'ordonnance du Conseil fédéral y relative.

Selon le Département fédéral de justice et police, ce système a été conçu comme un système fermé, c'est-à-dire qu'il n'est relié à aucun autre système d'information et que seule l'actuelle police fédérale du Ministère public de la Confédération (dans le futur: Office fédéral de la sûreté intérieure) est habilitée à l'utiliser. Il convient toutefois de relever que l'ordonnance ISIS prévoit la possibilité d'autoriser certains agents de l'Office fédéral de la police à consulter certaines données du système. En outre, le projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure prévoit que les personnes appartenant aux services de sûreté de la Confédération ainsi que des cantons et exerçant des tâches définies par cette loi auront un accès online à ce système informatique. Indépendamment de ce projet de loi, nous avons été contactés par le Ministère public de la Confédération pour examiner les conditions juridiques qu'il conviendrait de remplir pour la mise en place prochaine d'accès online des cantons au système provisoire ISIS.

ISIS a été élaboré en tant que système provisoire. L'ordonnance y relative est ainsi applicable uniquement jusqu'à la mise en service définitive d'ISIS mais au plus tard jusqu'au 31 décembre 1996. Nous avons régulièrement soutenu au cours des différentes phases d'élaboration d'ISIS qu'il conviendra, dans la perspective de la mise en place d'un système informatique définitif, de vérifier le fonctionnement des mécanismes relatifs à l'effacement des données, d'examiner la justesse des différentes durées de conservation et de régler les conditions du raccordement online des organes de sûreté des cantons au système.

En ce qui concerne le droit d'accès des individus, la réglementation actuellement en vigueur prévue dans l'ordonnance ISIS correspond aux dispositions de la loi fédérale sur la protection des données. Il conviendra cependant de voir les résultats des débats parlementaires portant sur l'examen du projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure adopté par le Conseil fédéral le 14 mars 1994. Ce projet, à l'instar de celui relatif à la création d'un office central de lutte contre le crime organisé, prévoit en effet l'introduction d'une disposition plus restrictive sur l'exercice du droit d'accès. L'avant-projet qui nous avait été soumis dix mois auparavant pour prise de position contenait une disposition adéquate renvoyant pour ce qui concerne l'exercice du droit d'accès à la loi fédérale sur la protection des données. Bien que le droit d'accès constitue la pierre angulaire de la protection des données, nous n'avons, en dépit de nos demandes réitérées et de nos craintes de voir l'option choisie pour le crime organisé reprise pour la sécurité intérieure, pas été consultés sur l'introduction d'une nouvelle norme plus restrictive dans le projet de loi.

Comme déjà mentionné dans le chapitre consacré à la création d'un office central de lutte contre le crime organisé, cette norme restrictive sur le droit d'accès, en faisant dans un premier temps référence à la LPD, garantit que chaque demande devra être examinée en procédant à une pesée concrète des intérêts en présence et en tenant compte du principe de la proportionnalité. Cependant la norme prévoit ensuite une série d'exceptions à la LPD. Nous reconnaissons la pertinence de la possibilité de ne pas motiver une restriction du droit d'accès dans les cas où la divulgation des renseignements pourrait compromettre l'objectif visé par la décision de restriction. L'obligation d'invoquer un intérêt particulier peut à la rigueur être justifiée dans le cadre spécifique des mesures visant au maintien de la sûreté intérieure, bien qu'elle se heurte à la jurisprudence du Tribunal fédéral qui 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. Par contre, la condition imposée à la personne concernée de se référer à un état de faits concret n'est 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'autoaccuser 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 par la police d'une surveillance abusive ou infondée. Nous estimons donc qu'en regard du respect des droits fondamentaux et de la personnalité des individus, cette dernière condition devrait être supprimée. Il appartiendra au Parlement de trancher.

Il nous apparaît encore important de relever que les concepteurs du projet de loi fédérale sur des mesures visant au maintien de la sûreté intérieure justifient l'introduction d'une telle réglementation restrictive en matière de droit d'accès en faisant référence au droit allemand. Ainsi, le Message relatif à ce projet de loi précise que "*cette solution, que nous avons également proposée pour le système d'information de l'office central en matière de lutte contre le crime organisé (...) a d'ailleurs fait ses preuves comme règle de droit germanique pour l'octroi de renseignements à l'Office fédéral allemand de protection de la Constitution*". Or il convient de signaler que précisément cette solution entrée en vigueur en Allemagne en décembre 1990 a, lors de son adoption, fait l'objet également d'oppositions en Allemagne même et qu'après quelques années d'expérience, elle reste toujours sous le feu de la critique! Ainsi, à l'instar de nos propres réserves, le Délégué fédéral

allemand à la protection des données a, dans le cadre de ses 13e et 14e rapports d'activité de 1991 et 1993, émis de vives critiques à l'encontre de cette solution tant sur son principe même que sur son application par trop restrictive.

Pour ce qui concerne les autres remarques que nous avons émises sur l'avant-projet de loi qui nous a été soumis, il convient de relever que certaines ont été retenues avec succès. Ainsi, nous avons demandé à ce que les accès online de certaines autorités au système informatique soient expressément prévus dans la loi, qu'ils tiennent compte du principe de proportionnalité et qu'ils soient limités aux seules autorités qui en ont réellement l'utilité et qui traiteront les données dans le même but que celui indiqué lors de leur collecte. Dès lors, selon le projet de loi, la banque de données relative aux mesures visant au maintien de la sûreté intérieure ne sera accessible non pas à n'importe quelle autorité fédérale ou cantonale mais uniquement aux services de sûreté de la Confédération et des cantons chargés des tâches définies dans la loi sur la sûreté intérieure. Il conviendra toutefois d'examiner dans le détail quels sont ces services.

2. Droit des étrangers et droit d'asile

2.1. Registre automatisé des personnes AUPER-2

Peu de mois avant le début de la période couverte par ce rapport, c.-à-d. le 1er janvier 1993, le registre automatisé des personnes AUPER-2 fut mis en service. Ce système est utilisé entre autres par l'Office fédéral des réfugiés et les autorités cantonales de police des étrangers pour traiter les données sensibles des requérants d'asile et des réfugiés. Il est également mis à la disposition d'autres organes, parmi eux des organes qui s'occupent en premier lieu de rechercher des personnes. Pendant la période couverte par ce rapport, il a été nécessaire à plusieurs reprises de contester le fait que le système AUPER-2 permet, en raison de sa réglementation généreuse en matière d'accès, d'effectuer des traitements de données pour lesquels la base légale requise manque ou qui sont enclins à porter atteinte à la personnalité d'un grand nombre de personnes. Malheureusement les efforts de la protection des données ont été sérieusement compromis par le manque de coopération parmi les responsables du système. La première mesure qui s'impose est d'obtenir une image claire de l'état actuel de ce système qui est en constante évolution. Ensuite, il sera nécessaire d'émettre des recommandations contraignantes pour améliorer et développer les mesures de protection des données et pour les appliquer.

Le 30 janvier 1992, la direction générale du projet AUPER-2 a décidé, à la demande de la protection des données, de rédiger un rapport visant à éclaircir les questions de sécurité et à établir de meilleures bases pour une nouvelle ordonnance AUPER, dont la rédaction nous fut confiée. Après d'intenses discussions avec les responsables du système et après avoir entendu également à plusieurs reprises les utilisateurs du système, ce rapport fut achevé le 7 octobre 1992, puis soumis à la direction générale du projet. Ce rapport ne prétendait pas faire une analyse exhaustive de la situation actuelle, ni évaluer les problèmes de sécurité du système AUPER-2 peu avant sa mise en service. Ceci aurait nécessité la participation d'experts externes, fait qui a été reconnu par la direction générale du projet et mentionné dans le rapport. Malgré cela, divers vices, en partie graves, ont pu être mis en évidence et des propositions ont été faites pour y pallier. Figure en premier plan la proposition de séparer

strictement les données des organes de police (pour la recherche de personnes) et les données relatives aux requérants d'asile dans AUPER-2, tant au niveau du stockage des données qu'à celui de l'octroi des accès, afin d'éviter que les données des requérants d'asile ne puissent être utilisées de manière incontrôlée par les organes de police en plus de leurs propres données, pour toutes sortes de tâches policières en Suisse et à l'étranger. Ceci est d'autant plus important que la majorité des utilisateurs de systèmes informatiques centralisés tels qu'AUPER-2 disposent de leurs propres systèmes bureautiques et de connexions de «courrier électronique», aussi avec l'étranger. D'autre part, seules les données des requérants d'asile vraiment nécessaires pour l'accomplissement de la tâche légale devraient être enregistrées de manière électronique et mises à disposition, ce qui (d'après les résultats des auditions) n'est pas toujours le cas dans AUPER-2. Ces défauts, ainsi que quelques autres, ont également été soulignés lors de la procédure de consultation des offices relative à l'ordonnance AUPER du 18 novembre 1992. Nous avons indiqué clairement que notre accord dépendait du fait que ces problèmes fussent réglés avant ou peu après la mise en service du système AUPER-2, respectivement de l'entrée en vigueur de l'ordonnance AUPER. Après que la direction générale du projet eut promis de pallier ces défauts, nous avons donné notre accord à la mise en exploitation d'AUPER-2 et à l'ordonnance AUPER. Malheureusement par la suite, on força le développement du système AUPER-2 plutôt que de régler, comme promis, les problèmes soulevés.
C'est pourquoi nous avons recommandé, après une analyse complète de la situation actuelle d'AUPER-2, de séparer de manière conséquente les données des requérants d'asile et des réfugiés des autres données personnelles d'AUPER-2 et de limiter au strict minimum les traitements effectués par les organes de police avec des données relatives aux requérants d'asile et aux réfugiés. La procédure est encore pendante.

2.2. Registre central des étrangers RCE

Le registre central des étrangers RCE de l'Office fédéral des étrangers contient les données les plus diverses concernant environ 3,5 millions d'étrangers ayant séjourné ou séjournant encore en Suisse. Un grand nombre d'autorités de la Confédération, des cantons et des communes utilisent ces données. Le système est en constant développement. Malheureusement nous avons dû prendre connaissance que des organes de police ont à plusieurs reprises eu un accès online à ces données sans aucune autorisation ni base légale. Ceci s'est à nouveau produit très récemment. D'autre part, il semble que les données traitées sont souvent mal protégées et qu'une partie d'entre elles n'est pas (ou ne peut pas être) mise à jour. C'est pourquoi il s'impose également de procéder à une analyse complète de l'état actuel du système RCE, puis de définir et d'appliquer les mesures nécessaires à l'amélioration et au développement de la protection des données dans ce système.

Au printemps 1992 nous avons appris que les postes frontière et les organes de police des cantons disposaient d'un accès online au système RCE, sans qu'ils y soient autorisés. Par une modification de l'ordonnance RCE, le Conseil fédéral donna l'autorisation expresse aux autorités désignées d'accéder directement au RCE pour accomplir des tâches clairement définies dans le domaine du droit des étrangers. La protection des données était assurée par des mots de passe et des profils d'accès. Par la suite, le système RCE fut soumis à un audit afin d'éviter que de tels incidents ne se reproduisent. Nous avons reçu un exemplaire du rapport final de cet audit,

rapport qui n'indiquait aucune raison justifiant une intervention immédiate de notre part. Pourtant, l'Office fédéral des étrangers, en qualité de maître du fichier RCE, nous pria de lui accorder notre assistance pour les questions relatives à la protection des données du RCE ou de prendre position quant à certaines questions ou mesures. Dans le cadre de cette activité, qui ne s'est terminée que dans la période couverte par ce rapport, nous avons donné de nombreux avis en matière juridique concernant des questions en rapport avec la protection des données. Nous avons également pris part à diverses réunions des responsables et des utilisateurs du système, avec l'assistance d'un spécialiste en informatique. Des démonstrations de traitements de données ont été également effectuées lors de ces réunions. Etant donné que le système RCE est en constant développement, il ne fut pas possible d'obtenir une image claire de l'état du système ni d'apporter un jugement définitif. D'autre part, l'audit mentionné précédemment n'ayant pas dévoilé certains problèmes majeurs de protection des données dans le système RCE (voir les explications à la fin du paragraphe suivant), une analyse systématique de l'état actuel et une appréciation au regard de la protection des données s'avèrent de plus en plus nécessaires et urgentes.

Dans le cadre des activités de conseil mentionnées ci-dessus, divers avis ont été rédigés sur les questions de base de la conception (''architecture'') d'un gros système informatique tel que le RCE. Un des avis portait sur la question de l'obligation de journaliser les accès illicites des organes de police aux données civiles. Un autre traitait des questions de sécurité des données dans les centres de calcul de la Confédération et des cantons, notamment dans le cas où des données en provenance de divers fichiers sont traitées et communiquées en un endroit central avec les mêmes équipements et de manière non cryptée. Un autre avis analysa les problèmes de liaisons de systèmes informatiques de la Confédération avec des systèmes des cantons, surtout lorsque des "données fédérales sensibles" doivent être transférées dans un environnement cantonal dans lequel les droits d'accès sont réglementés de manière souple. Notre activité s'est en deuxième lieu concentrée sur la communication dans le cadre de l'entraide administrative de gros volumes de données relatives à des étrangers aux autorités de police ou d'enregistrement de pays étrangers ainsi que de documents de visa aux polices cantonales ou de données concernant des étrangers ou l'assurance chômage aux autorités fiscales des cantons. Le troisième point crucial est la question du volume et de la nécessité de traiter les données par des moyens électroniques. Du point de vue de la protection des données, la conservation et la gestion de grandes quantités de dossiers souvent non structurés par des moyens électroniques, tel que cela est semble-t-il prévu avec le système informatique REGI-2 pour l'ensemble des dossiers de l'Office fédéral des étrangers, doivent être considérées comme problématiques. Déjà lors de la saisie électronique, les erreurs ne peuvent être exclues. D'autre part, les données sensibles et les profils de la personnalité ainsi enregistrés peuvent être alors traités et exploités par une multitude de moyens électroniques des plus variés. Etant donné que le cryptage est aujourd'hui souvent considéré comme trop astreignant, de gros risques de sécurité en découlent, ce qui pourrait engager d'importantes responsabilités. De même, la question de la licéité des champs libres (appelés aussi champs "mémo") et des codes de remarque dans le RCE ont fait l'objet d'une appréciation au regard de la protection des données. Il semble que les propositions qui ont été faites ont déjà pu être mises en pratique, c.-à-d. que le RCE n'utilise plus que des champs libres standardisés au contenu irréprochable d'un point de vue de la protection des données et des codes de remarque à valeur non

significative. - Le volume des données traitées dans le RCE fut en outre l'objet de divers entretiens avec les unités organisationnelles d'utilisateurs. Il s'avéra que les réglementations existantes des droits d'accès sont très rarement basées sur une véritable analyse des tâches et donc souvent trop généreuses. Lors des entretiens avec l'Office fédéral de la police fin 1993/début 1994, il s'avéra que cet office dispose apparemment de nombreux accès depuis plusieurs années au registre central des étrangers sans y être légitimé. Afin de pouvoir peser objectivement les intérêts des personnes concernées par rapport à la sécurité, nous devrions pouvoir examiner des documents tels que ceux qui résultent d'une analyse des tâches comme nous l'avons décrite ci-dessus. De tels documents font ici également défaut. Nous avons donc conseillé de réduire les traitements de données RCE par l'Office fédéral de la police à un strict minimum et de procéder immédiatement à une analyse des tâches. La procédure est encore pendante.

2.3. Révision de la loi sur l'asile et de la loi sur le séjour et l'établissement des étrangers (LSEE), protection des données et entraide judiciaire et administrative

Ont également eu lieu dans la période couverte par ce rapport les travaux préparatifs pour la modification de la Loi sur l'asile et de la Loi fédérale sur le séjour et l'établissement des étrangers, auxquels nous participons également. Selon les dispositions de la LPD, des traitements sensibles de données tels qu'ils ont lieu notamment dans le domaine de l'asile, mais également dans le domaine de la juridiction des étrangers doivent reposer sur une base légale appuyée par voie démocratique. Du point de vue de la protection des données, on peut se féliciter de voir que les dispositions qui manquaient jusqu'ici dans les domaines de l'asile et des étrangers sont en voie d'élaboration. Il est à souhaiter que ces dispositions s'orientent autant que possible sur les objectifs de la LPD. Il serait mal indiqué que des pratiques controversées de traitement des données soient ancrées dans la loi sans avoir été discutées à fond, simplement pour répondre aux exigences formelles. Un certain danger dans ce sens semble exister dans le secteur de l'asile et de la loi sur les étrangers du fait qu'un accès direct (online) aux données souvent sensibles est octroyé ou prévu de l'être sans qu'il existe pour cela une vraie nécessité. Une pratique qui nous semble également très douteuse au regard de la protection des données est l'échange incontrôlé de données de requérants d'asile notamment avec l'étranger, par exemple dans le cadre d'INTERPOL. D'autre part nous devons pour des raisons de protection de la personnalité et des données nous élever contre les procédés discriminatoires envers les requérants d'asile lors du prélèvement d'empreintes digitales.

Les organes fédéraux sont tenus de fournir une *entraide administrative*. L'article 19 LPD les autorise expressément à communiquer des données personnelles dans le cas d'une entraide administrative s'il existe une base juridique ou si le destinataire a dans un cas d'espèce absolument besoin de ces données pour accomplir sa tâche légale. Ils doivent cependant refuser la communication, la restreindre ou l'assortir de charges si des intérêts prépondérants ou des obligations légales de garder le secret ainsi que des dispositions particulières relevant de la protection des données l'exigent. Si quelqu'un obtient cependant un accès direct (online) aux banques de données électroniques d'un organe fédéral, il n'est plus possible à partir de ce moment de vérifier si les demandes individuelles sont vraiment nécessaires ou licites ou si elles devraient plutôt être refusées ou restreintes par l'organe fédéral. De tels accès directs ne sont donc admissibles que si l'on peut exclure a priori la possibilité

qu'un intérêt majeur, une obligation légale de garder le secret ou une disposition spéciale relevant de la protection des données puissent les empêcher. Ceci est très rarement le cas. Pour garantir que ce principe de base de la protection des données ne soit pas inconsidérément ignoré, la LPD exige une autorisation légale formelle pour de tels accès online, et pour la communication de données sensibles même une autorisation expresse dans une loi au sens formel. Si un tel accès online ne peut être accordé, ce qui pourrait être la règle, une entraide administrative est néanmoins possible dans la plupart des cas, à savoir si l'examen du cas et la situation juridique le permettent dans le cas d'espèce.

Fortement pressés par le temps et avec les réserves mentionnées ci-dessus dans le paragraphe relatif à AUPER-2, nous avons donné fin 1992 notre accord, sur requête de diverses autorités de police de la Confédération, à leur accès en ligne aux données des requérants d'asile mémorisées dans le système AUPER-2. Ces autorités avaient fait valoir la plupart du temps qu'elles devaient pouvoir savoir rapidement si une personne donnée avait déposé une demande d'asile. Entre-temps nous savons que ces autorités avaient à leur disposition des masques de recherche illimités et avaient accès à des données qui, en plus de l'objectif annoncé, permettaient de faire des recherches par quadrillage. D'autre part, ces autorités furent équipées entre-temps d'appareils modernes de bureautique, qui permettent de procéder à d'autres traitements incontrôlés de ces données et de les communiquer à l'étranger. Des accès du même type semblent également possibles ou au moins prévus sous peu dans le registre central des étrangers. Il semble également que nombre d'organes sont d'avis que des demandes d'INTERPOL concernant des données de requérants d'asile ou d'étrangers ne nécessitent pas de pesée des intérêts, tel que cela a été décrit, mais que selon les statuts d'INTERPOL les données requises doivent en tous les cas être communiquées, même aux pays ne disposant pas d'une protection des données suffisante. Les accès online ayant lieu dans ces conditions doivent être absolument refusés. Des dispositions légales formelles, telles qu'elles pourraient être proposées dans le cadre des révisions prévues et qui autoriseraient le traitement des données des réfugiés d'une manière si peu différenciée ne pourraient en aucun cas être approuvées autant au regard du droit constitutionnel qu'à celui de la protection des données. Nous avons clairement exposé ce point de vue au cours de la période couverte par ce rapport à diverses reprises et avons demandé à ce que l'ordonnance AUPER soit adaptée. Nous avons soumis des propositions concrètes qui visaient à permettre dans certains cas limités des accès online pour des interrogations individuelles, limitées au niveau du contenu, sans masques de recherche illimités et qui permettraient grâce à la journalisation d'éviter l'utilisation à des fins non prévues des données interrogées, notamment par des tiers. Jusqu'ici, ces propositions ont toutes été rejetées.

Lors d'un *échange de données à l'échelon international*, le pays destinataire doit disposer d'une protection des données au moins équivalente. La protection des données peut être considérée comme équivalente si le principe de la finalité est respecté lors du traitement des données et si d'une manière générale les données communiquées sont suffisamment protégées. Cela signifie, en d'autres mots, que l'on doit savoir a priori quelle autorité étrangère est responsable de réceptionner les données transmises et s'être assuré que celle-ci n'utilisera pas les données à des fins autres que celles prévues et qu'elle ne communiquera pas les données à autrui. Ces principes sont également valables selon l'article 15 de la convention de Dublin de 1992 sur le premier asile, qui règle en grande partie les compétences inter-

européennes lors du traitement des demandes d'asile ainsi que l'échange de données qui en résulte, et à laquelle la Suisse a adhéré dans le cadre d'une convention parallèle. Les données à transmettre sont clairement définies dans cet accord (catalogue des données), ce qui doit être respecté lors de l'élaboration de lois nationales, sous réserve d'éventuelles dérogations. L'accord exige également que l'échange de données soit journalisé. C'est pourquoi nous avons suggéré à plusieurs reprises de prévoir notamment dans la loi sur l'asile révisée des prescriptions concernant l'affectation à un but précis et à une autorité précise tel que cela a été expliqué plus haut de même qu'un catalogue des données de requérants d'asile qui peuvent être communiquées à l'étranger. - Dans cet ordre d'idées, les dispositions de la convention complémentaire de Schengen de 1990 (qui sont pratiquement les mêmes dans le domaine de l'asile) sont également d'importance. Selon cet accord, le nouveau système d'information de Schengen qui est prévu ne pourra pas - en plus des données du secteur policier - traiter ou stocker des données de demandeurs d'asile. Ceci concrétise le principe de finalité déjà évoqué, qui est également important pour le droit suisse. La transmission des empreintes digitales - souvent utilisées dans le cadre de poursuites policières - n'est pas réglementée dans le droit international des réfugiés discuté ici. D'un point de vue de la protection des données, cette transmission semble être plutôt problématique (intensité de l'atteinte, effet discriminatoire et caractère sensible des données). Nous avons déconseillé de communiquer de telles données de requérants d'asile non criminels à l'étranger. Si une telle communication devait s'avérer incontournable, les données devraient être bien protégées et communiquées à une autorité d'asile qui ne conserve pas ces données avec les données pénales.

Avec *la révision de la loi sur l'asile*, il semble qu'il soit prévu d'intégrer le régime transitoire actuel dans le droit ordinaire, ce qui signifierait que les empreintes digitales doivent être prélevées pour tous les requérants d'asile sans exception, puis enregistrées dans le système automatique d'identification des empreintes digitales AFIS du Ministère public de la Confédération et de l'Office fédéral de la police. Nous avons instamment fait savoir à plusieurs reprises que le prélèvement des empreintes digitales ne doit être que l'ultime recours. C'est pourquoi le texte de la loi sur l'asile devrait être formulé de manière à être compatible avec l'art. 351quinquies du code pénal. D'autre part, la conservation commune des données des requérants d'asile avec celles des criminels doit être strictement rejetée pour les raisons de protection des données indiquées précédemment. Lors d'une démonstration du système AFIS, il s'est pourtant avéré que les formulaires contenant les empreintes digitales sont munis d'un numéro d'identification qui n'est pas lié à la personne, mais également que les autorisations d'accès et de traitement ainsi que les mesures de sécurité ne sont absolument pas conformes à la protection des données. C'est pourquoi les objections faites au nom de la protection des données doivent être maintenues dans leur intégralité.

2.4. Autres activités dans les domaines du droit d'asile et du droit des étrangers

Ont également eu lieu pendant la période couverte par le présent rapport les prises de position relatives aux *accords avec l'Allemagne et la Hongrie concernant la reprise de personnes à la frontière* ainsi que nos avis relatifs à l'accord de Schengen-Pologne de même contenu. Dans ces cas, nous avons malheureusement été informés très tard de certaines démarches décisives. Il fut néanmoins possible de

suggérer l'inclusion dans les accords avec l'Allemagne et la Hongrie des principes de base décrits ci-dessus concernant l'affectation à une utilisation et une autorité lors des échanges internationaux de données et l'élaboration d'un catalogue des données liant les parties. Dans le cas de l'accord avec l'Allemagne, nous avons en outre procédé à une enquête sur les traitements de données aux frontières et dans les aéroports suisses, enquête qui nous a livré les bases nécessaires. Dans un autre contexte, nous avons eu la possibilité d'être confrontés à des questions de protection des données dans le domaine de la santé et de l'assistance aux requérants d'asile et de les discuter en détail (co-rapport concernant le projet informatique LIFAS).

3. Télécommunications

3.1. L'annuaire X.500 (X.500-Directory): un système d'information à l'échelle mondiale

L'annuaire X.500 est un système d'information à l'échelle mondiale, permettant aux personnes et institutions raccordées au système dans le monde entier de consulter des informations stockées dans cet annuaire. Actuellement un projet pilote est en cours, auquel participent 30 pays avec plus d'un million d'enregistrements de données. La disponibilité à l'échelle mondiale de l'annuaire X.500 ainsi que la possibilité qu'il offre de combiner des données personnelles posent de gros problèmes du point de vue de la loi sur la protection des données.

Toute communication repose sur un échange d'informations. Pour chaque échange d'informations, l'expéditeur d'un message a besoin de connaître l'adresse du destinataire. Cette adresse peut être une adresse postale ou un numéro de téléphone. Si nous transposons cet état de fait dans le monde de la transmission électronique des données, nous nous rendons compte que nous avons également besoin d'informations permettant de nous adresser à un partenaire avec lequel nous pouvons communiquer. Il s'avère cependant que les adresses utilisées dans ce domaine ne sont souvent pas aussi compréhensibles et familières que ne l'est une adresse postale.

Il existe aujourd'hui un grand nombre d'annuaires (par ex.: numéros de téléphone, numéros de téléfax, adresses X.25, adresses X.400,...), qui souvent contiennent des données redondantes. D'autre part, ces annuaires sont disponibles dans les environnements de systèmes les plus variés et sur des supports de types très différents. Si une information est modifiée, cela nécessite une mise à jour de tous les annuaires dans lesquels cette information est contenue. Prenons l'exemple d'un changement de domicile. Rien que d'informer tous les organes concernés qu'ils doivent modifier l'adresse est déjà un grand effort qui, de surcroît, ne mène souvent pas au succès attendu, un grand nombre d'erreurs étant souvent faites. Si l'on pense à la transmission électronique des données, on se rend compte qu'une erreur dans ce domaine peut avoir des conséquences graves. Ceci fut une des motivations majeures pour désirer disposer d'un annuaire toujours à jour, facile à entretenir et accessible à tous les intéressés.
C'est pourquoi on a créé une norme pour un annuaire (Directory-Standard) qui devrait permettre de mettre à jour aisément les informations enregistrées.
Cette norme a été élaborée et décrite par le CCITT (Comité Consultatif International Télégraphique et Téléphonique) et l'ISO (International Organisation for

Standardization). Ces normes sont connues sous l'appellation X.500 et suivantes pour le CCITT, ainsi qu'ISO - 9594 - 1 à 8 pour ISO.

Ce service (X.500 ou ISO 9594) permet de rendre accessibles de manière globale des informations relatives à des objets variés dans un environnement de communication réparti (personnes, organisations, autres services ou ordinateurs, etc.). Le service d'annuaire selon X.500 gère, en principe indépendamment des applications, l'enregistrement d'informations dans une base de données appelée Directory Information Base (DIB) ainsi que sa structure logique. Il définit également les règles de maintenance et l'accès à ces informations par le biais de protocoles d'accès standardisés. Chaque entrée dans la DIB est identifiée par un nom. Chaque élément d'une DIB doit être désigné de manière unique dans le monde entier. Les instances attribuant les noms doivent disposer de compétences clairement définies.
Etant donné qu'X.500 permet de définir la structure logique des données, il est possible par ce moyen de gérer presque chaque type d'information. Ainsi on peut enregistrer les données aussi bien à des fins d'adressage que pour se procurer des informations. Comme exemple, nous pourrions citer l'élaboration d'un annuaire téléphonique (pages blanches et jaunes) aussi bien que celle d'un catalogue de vente par correspondance. Selon les moyens techniques, les informations peuvent contenir, en plus du texte, des images ou des sons. Les données peuvent être stockées et gérées de manière distribuée. L'accès aux données a lieu au moyen de demandes de recherche. Il existe des moyens de restreindre l'accès individuel à un objet.

En Suisse, c'est le SDF (Swiss Directory Forum) qui est chargé de la mise en place des services d'annuaire selon X.500. Ici, tant la question de l'inclusion à l'échelle mondiale que celle de l'utilisation en Suisse sont intéressantes. Ce forum s'occupe actuellement de définir et de réglementer les responsabilités pour l'attribution des noms ainsi que de définir la structure DIT (Directory Information Tree) pour la Suisse. Nous avons la possibilité de collaborer depuis fin 1993. La question centrale est celle de définir les informations à rendre accessibles dans le Swiss Directory et d'évaluer les points qui ont un impact sur la protection des données et qui devraient être réglés.

A l'origine, l'idée de l'annuaire X.500 fut de permettre à des sociétés de mettre à tout moment à disposition de leurs partenaires commerciaux les noms, adresses, numéros de téléphone et de téléfax ainsi que "l'identification courrier électronique (E-Mail)" de leurs collaborateurs, et ce à l'échelle mondiale. Comme cela est souvent le cas, ce projet développa sa propre dynamique avec pour résultat que les informations disponibles aujourd'hui par X.500 ne se limitent plus aux informations de télécommunication des entreprises. Vu que nombre de personnes privées ont fait part de leur intérêt à exploiter X.500 pour leur propres buts, il est aujourd'hui possible de consulter toutes sortes de données, de contenu et de forme très variés, par le biais de X.500: passages de texte à des fins scientifiques, noms, adresses, numéros de téléphone et de téléfax, identifications E-Mail, professions, fonctions, images - que ce soient des images d'objets, des portraits de personnes ou des empreintes digitales -, des séquences sonores -telles que de la musique, mais aussi des voix -, les passe-temps, couleur des cheveux, boissons préférées, mensurations, etc. etc.

Du point de vue de la protection des données, *la disponibilité de données personnelles à l'échelle mondiale* par ordinateur pose de gros problèmes, étant

donné que tout ce qui a été introduit dans le système peut en principe être consulté par quiconque est connecté au X.500. Les données stockées dans le système ne peuvent donc pas seulement être consultées dans la sphère d'influence de la loi suisse sur la protection des données, mais également dans d'autres pays européens et même extra-européens ne disposant pas d'une législation sur la protection des données équivalente à la nôtre. La conséquence en est que la protection de la personnalité dans les divers pays ne correspond pas aux exigences de la LPD suisse, ce qui peut avoir des conséquences graves pour la personne concernée, notamment lorsque des données sensibles ou des profils de la personnalité sont mis à disposition.

Un autre point très important sous l'angle de la protection des données est *la possibilité d'interconnecter les données*. Ceci ne concerne pas seulement les données sensibles et les profils de la personnalité qui sont directement mis à disposition dans le système. Ce problème touche également les données personnelles "normales" qui, à l'aide de l'ordinateur, deviennent disponibles et peuvent être combinées de manière incontrôlée. Ainsi, il est possible, à partir de données personnelles absolument "normales", de générer des profils de la personnalité, mais également de traiter ces données à des fins incontrôlables. On relèvera que des données personnelles sont pourtant déjà contenues dans des annuaires imprimés, données qui, dans ce contexte, ne sont pas sensibles, ni constitutives de profils de la personnalité. La combinaison de ces données en provenance de plusieurs annuaires pour en créer des profils de la personnalité constituerait une tâche énorme, voire impossible. Avec X.500 en revanche, la combinaison de ces données disponibles peut être accomplie aisément, avec une vitesse absolument fascinante et sans gros efforts.
Une des approches techniques possibles pour résoudre le problème de l'interconnectabilité pourrait être un contrôle d'accès très poussé.

Afin de tenter de résoudre au moins en partie les problèmes exposés, il est nécessaire d'une part d'élaborer et d'offrir aux fournisseurs suisses d'informations des réglementations aussi unifiées que possible, d'autre part d'élaborer des directives communes d'utilisation de X.500 sur un plan international ou au moins européen.
Dans le cadre de la juridiction suisse, les approches suivantes pourraient être envisagées:
créer une sorte de contrat pour *les fournisseurs privés d'informations*, contrat qui règlerait les conditions et les modalités de la mise à disposition de données personnelles ainsi que d'autres responsabilités, telles que déterminer les données personnelles pouvant être rendues accessibles, veiller à ce que des sociétés ne mettent pas à disposition de données sensibles ou de profils de la personnalité de leurs collaborateurs et à ce que des données personnelles de tiers (collaborateurs, etc.) ne puissent être rendues accessibles qu'avec le consentement préalable écrit de la personne concernée, attirer l'attention sur l'éventuelle insuffisance de la protection de la personnalité offerte dans d'autres pays ou Etats, ainsi que sur les conséquences juridiques, etc.
Ce règlement devrait être signé par toute personne abonnée à X.500.

Etant donné que *des organes fédéraux* peuvent également mettre à disposition des données personnelles, autant sur eux-mêmes que sur autrui (collaborateurs, etc.), il est nécessaire d'entreprendre l'élaboration d'une loi obligatoire pour tous les organes

fédéraux, dans laquelle il faudrait définir les données personnelles pouvant être rendues accessibles et à quelles conditions (consentement, conditions techniques, etc.).
On pourrait également envisager de fixer des conditions obligatoires que tout bénéficiaire de liaison à X.5oo octroyée par l'OFCOM devrait signer, quel que soit son statut X.500 (personne privée, organe fédéral ou cantonal), cette signature étant une condition préalable à l'octroi d'un tel accès et signifiant l'acceptation de ces conditions.

3.2. Surveillance des fréquences

Suite à une intervention de notre part après information préalable par la presse, un groupe de travail a été mis sur pied qui est chargé d'élaborer une base juridique suffisante pour les surveillances de fréquences effectuées par les PTT, au cours desquelles ceux-ci écoutent et enregistrent le contenu des conversations tenues au moyen de téléphones sans fil.

Après avoir analysé les faits sous l'angle de la protection des données et du droit constitutionnel, nous avons fait part aux médias de notre constatation selon laquelle il n'existe pas de base juridique suffisante sous forme de loi au sens formel pour justifier une telle pratique.
Un groupe de travail a par la suite été constitué, ayant pour mandat de créer une telle base légale.
De notre point de vue, les objectifs de la disposition à élaborer doivent être les suivants: définir dans quels buts une surveillance des fréquences peut avoir lieu, fixer les conditions auxquelles l'écoute et/ou l'enregistrement du contenu des conversations tenues sur la fréquence sont admissibles, réglementer les conditions de la communication de données personnelles collectées par ce moyen à l'OFCOM ou aux autorités fédérales de poursuite pénale, etc.

Le groupe de travail comprend des représentants de l'OFCOM, de la direction générale des PTT, du Tribunal fédéral et de nos services. Entre-temps, notre avis concernant l'absence de base légale a été confirmé par un document de travail interne élaboré par un représentant du Tribunal fédéral.

3.3. Surveillance des téléphones/observation à des fins de poursuites pénales

Sur la base d'un rapport remis par la commission de gestion du Conseil national et de l'avis du Conseil fédéral qui s'en est suivi, le conseiller fédéral Koller a décidé de mettre sur pied un groupe de travail Surveillance téléphonique. Ce groupe est chargé d'élaborer une réglementation plus stricte concernant la surveillance téléphonique, valable également pour les cantons et offrant une protection accrue de la personnalité. De même, il devra proposer de nouvelles dispositions pour réglementer l'observation et l'engagement d'agents infiltrés. Parmi les 14 membres du groupe figure un seul représentant de la protection de la personnalité/des données.

La commission de gestion du Conseil national (CdG Conseil national) a rédigé le 9 novembre 1992 un rapport intitulé "Surveillance téléphonique dans la Confédération", dans lequel elle demande d'élaborer une réglementation plus stricte concernant la surveillance téléphonique aux fins de poursuites pénales ainsi que de nouvelles

dispositions réglementant l'observation et l'engagement d'agents infiltrés, dispositions qui seraient en accord avec la réglementation concernant la surveillance téléphonique. Le Conseil fédéral a pris position sur ce rapport le 17 février 1993. Sur la base de ces constatations, le chef du Département fédéral de justice et police, le conseiller fédéral Koller, prit la décision de former le groupe d'étude Surveillance téléphonique. Ce groupe d'étude est chargé:

- d'élucider la question de la divulgation de données non publiées concernant les conditions d'un abonnement;
- de clarifier les besoins en législation, tels qu'ils ressortent de l'avis du Conseil fédéral du 17 février 1993 concernant le rapport de la CdG du Conseil national;
- d'élaborer un projet pour la procédure de consultation fondé sur les résultats des délibérations des Chambres (93.3205, motion de la CdG du Conseil national du 24 mai 1993. Surveillance téléphonique);
- de déterminer si l'élaboration d'un acte législatif spécifique ("loi fédérale sur les restrictions du secret des télécommunications") est préférable à une révision du code pénal suisse et d'autres lois fédérales;
- de déterminer si des prescriptions en matière de procédure pénale doivent être faites aux cantons sur la base du droit fédéral;
- de déterminer dans quelle mesure il est nécessaire d'élaborer une réglementation concernant la surveillance téléphonique dans le cadre de l'entraide judiciaire.

La motion 93.3205 de la CdG du Conseil national du 24 mai 1993, approuvée par le Conseil fédéral le 14 juin 1993, contient des propositions concrètes, telles que la création d'un catalogue restrictif de délits, complété par une clause générale, une meilleure protection des tiers, surtout des bénéficiaires du droit de refuser de témoigner, un contrôle a posteriori de l'efficacité et la procédure à suivre pour ordonner une observation ou l'intervention d'agents infiltrés.

Selon l'agenda prévu dans la décision, le groupe d'étude doit présenter son projet d'ici fin mars 1994. Si l'on tient compte du fait que la première séance préparatoire interne à l'administration a eu lieu fin octobre 1993, on est forcé de constater que le temps mis à disposition est bien trop court pour maîtriser un sujet si important et si délicat.
Certes, la révision du code pénal crée des dispositions obligatoires égales pour les cantons et la Confédération en ce qui concerne les conditions préalables et les procédures de surveillance téléphonique. Les projets élaborés, qui règlent l'engagement des moyens techniques de surveillance de la même manière que la surveillance téléphonique elle-même, présentent cependant le danger que le contenu essentiel de lois fondamentales soit affecté de manière inacceptable si l'on n'énumère pas au moins dans les notes explicatives quelles sont les mesures permises et celles qui ne le sont pas, par ex. lors d'implantation d'émetteurs sur le corps de personnes contre leur gré, de la pause de mouchards dans des appartements, de l'installation de caméras cachées dans des appartements.

D'autre part, une réglementation satisfaisante de l'observation et de l'engagement d'agents infiltrés doit être prise en main. Il faudra donc attendre l'évolution future.

..

3.4. La protection des données dans le domaine des télécommunications

Le domaine des télécommunications comprend une multitude d'équipements techniques permettant la communication d'un homme à un autre, de l'homme avec l'ordinateur et des ordinateurs entre eux. Avec le degré croissant de technicité et de complexité de la mise en réseau, on découvre de plus en plus d'offres, de constellations et de situations qui peuvent poser problème du point de vue de la protection des données et qui doivent être analysées.

Nous allons dans ce qui suit nous limiter à attirer votre attention sur un nombre restreint de cas actuels que nous rencontrons dans la vie de tous les jours.

Téléphone RNIS
Les PTT offrent un téléphone RNIS disposant d'un affichage. Cet affichage permet à l'appelé de voir quel abonné (numéro de téléphone) l'appelle, indépendamment du fait qu'il réponde à l'appel ou non. Ce numéro de téléphone de l'appelé s'affiche également si l'appelant est abonné à SwissNet, mais aussi si l'appelant a un appareil analogique, mais que la liaison a été établie par l'intermédiaire d'une centrale numérique des PTT.
L'appelant qui est lui-même abonné à SwissNet sait que son numéro d'abonné est affiché sur l'appareil de la personne appelée. Par contre, l'appelant qui possède encore un appareil analogique ne sait pas, en règle générale, qu'il est possible que son numéro d'abonné s'affiche sur l'appareil du destinataire. Le fait que ce numéro s'affiche peut offrir beaucoup d'avantages à l'appelé, avantages qui doivent d'un autre côté être confrontés à de sérieuses objections d'un point de vue de la protection des données:

- pour certaines institutions, l'anonymat de l'appelant constitue un principe de base de leur activité. Ceci est notamment le cas pour les autorités de la sécurité intérieure, la main tendue, les associations d'aide au malades du SIDA ou aux toxicomanes, etc.;
- l'appelé est en mesure d'enregistrer les numéros et de les dépouiller à des fins commerciales;
- il peut arriver que le numéro affiché sur l'appareil soit vu de la part de tierces personnes se trouvant dans l'entourage de l'appelé sans que celui-ci le veuille.

D'un point de vue de la protection des données il faut pouvoir assurer par des mesures techniques que l'affichage du numéro puisse être bloqué de manière individuelle par l'appelant. Cette possibilité n'existe pas encore, mais selon les PTT elle est prévue pour 1995.

L'enregistrement de conversations téléphoniques dans des centraux d'entreprise
Pour des raisons de coûts, de plus en plus d'entreprises installent leur propre central téléphonique manuel ou assisté par ordinateur. Grâce à ces centraux, ils enregistrent les conversations sortantes des employés, souvent même aussi bien les conversations sortantes qu'entrantes.
Le fait d'enregistrer un numéro d'appel peut, par les déductions possibles pouvant être faites sur les contacts téléphoniques d'une personne, mener à des atteintes à la personnalité. Cet enregistrement n'est donc admissible que s'il peut être justifié. Une des raisons permettant de justifier un tel enregistrement, pour un employeur notamment, peut être une raison d'organisation interne.
Une des conditions préalables pour que des numéros d'appel puissent être enregistrés au sein d'une entreprise est que les personnes concernées en soient informées à l'avance, et de manière substantielle.

D'autre part, il s'impose de vérifier la conformité du traitement de données effectué aux principes de la protection de la personnalité , eu égard au volume des données enregistrées:
nous sommes d'avis que - dans une certaine mesure - ces enregistrements peuvent être compréhensibles et défendables. Ainsi l'enregistrement de la date, du numéro de poste interne utilisé pour l'appel, de la durée de la conversation ainsi que du numéro appelé - pour autant qu'il ne soit pas possible d'en déduire qui est la personne appelée - est acceptable. On part du principe qu'il n'est plus possible de déduire qui est la personne appelée, lorsqu'on supprime les 4 derniers chiffres du numéro composé. De notre côté, nous proposons de limiter le numéro à l'indicatif, dans la mesure bien sûr ou cela est suffisant.
Le numéro complet de l'appelé ne peut être enregistré que si les mesures qui devraient être prises pour bloquer cet enregistrement ne peuvent être raisonnablement imposées et que l'atteinte à la personnalité de l'employé causée par l'enregistrement du numéro d'appel peut être justifiée par le but de cette atteinte.
L'enregistrement des numéros d'appel de l'employé et des destinataires des conversations privées faites au sein de l'entreprise à titre de contrôle représente une atteinte à la personnalité de l'employé. Il ne peut être effectué que s'il a été précédé d'une directive de l'employeur annonçant que les conversations privées au sein de l'entreprise sont interdites ou ne sont tolérées que dans une certaine mesure, et s'il n'existe pas de moyen moins incisif pour faire appliquer cette directive (par exemple en n'enregistrant qu'une partie du numéro appelé). Dans ce cas, les employés doivent avoir la possibilité, pour les cas urgents et pendant les pauses, de téléphoner à l'extérieur depuis un appareil non surveillé. En outre, les employés doivent être informés de manière détaillée sur les enregistrements prévus.
L'enregistrement de telles données pour les conversations professionnelles uniquement constitue une atteinte moindre à la personnalité des employés. Ceux-ci doivent néanmoins être préalablement informés du fait que ces enregistrements sont effectués. D'autre part, l'employé doit avoir lui-même la possibilité de bloquer l'enregistrement des conversations privées.
Dans le cas de l'enregistrement du contenu des conversations sortantes ainsi que dans le cas de l'enregistrement des conversations entrantes, les participants à la conversation doivent être préalablement informés qu'un enregistrement a lieu. A notre avis, ceci vaut également pour ce qu'on appelle les communications suédoises dans le secteur bancaire (ex.: les ordres de bourse donnés par téléphone).
Il faut veiller en tout temps à ce que les données enregistrées ne soient accessibles qu'aux seules personnes chargées de les dépouiller. Ce groupe de personnes doit rester aussi restreint que possible. En particulier, il faut éviter que les données soient imprimés en un lieu accessible publiquement.
Même si les enregistrements sont admissibles selon les principes énoncés ci-dessus, ils doivent être détruits après un certain temps. Si les enregistrements ne sont effectués qu'à des fins de contrôle, l'employeur est tenu de les analyser régulièrement, de prendre les mesures qui s'imposent puis de détruire immédiatement les enregistrements.

Codes et mots de passe pour les numéros 156
Dans le domaine des numéros 156 ("messageries roses"), des codes et mots de passe ont été introduits dans le but de protéger la jeunesse, ce qui doit en principe être salué. Nous devons cependant attirer l'attention sur le fait que l'introduction de codes ou de mots de passe peut, selon le moyen technique mis en oeuvre et selon la procédure utilisée, poser des problèmes de protection des données.

4. Statistique

4.1. Nouvelle loi sur la statistique fédérale (LSF)

La nouvelle loi sur la statistique fédérale réglemente désormais de manière uniforme la multitude de compétences permettant d'ordonner les relevés statistiques. L'ordonnance du 30 juin 1993 concernant l'exécution des relevés statistiques fédéraux énumère en annexe tous les relevés statistiques et arrête la liste des organes responsables de ces relevés en précisant leurs conditions de réalisation. Les dispositions requises en matière de protection des données figurent également dans cette loi, qui prévoit entre autres expressément la possibilité pour l'Etat d'intervenir dans la sphère personnelle en recueillant des renseignements. Elle constitue donc à ce propos un facteur de transparence.

Les statistiques établies par l'Office fédéral de la statistique à partir des données livrées par les autorités et les particuliers sont de plus en plus importantes. En effet, dans une société industrielle démocratique, la statistique officielle est essentielle à l'information sur la population, l'économie, la société et l'environnement.
Comme toutes les tâches de l'Etat, la statistique officielle doit également être étayée par une base légale répondant aux nécessités actuelles. L'ancienne base légale applicable (la loi fédérale du 23 juillet 1870 concernant les relevés officiels statistiques en Suisse) était très générale. Elle réglait uniquement la compétence d'ordonner les relevés et la participation des cantons aux frais, ainsi que la possibilité d'obliger les cantons à participer à l'élaboration de la statistique fédérale. Désormais, la nouvelle loi sur la statistique fédérale réglemente de manière uniforme la multitude des compétences permettant d'ordonner des relevés statistiques. Pour sa part, l'ordonnance du 30 juin 1993 concernant l'exécution des relevés statistiques fédéraux répertorie en annexe tous les relevés statistiques et arrête la liste des organes responsables de ces relevés, en précisant les conditions de réalisation de ces derniers.
Les dispositions requises en matière de protection des données figurent aussi dans cette base légale. Celle-ci réglemente notamment la possibilité pour l'Etat d'intervenir dans la sphère privée en recueillant des renseignements. Elle constitue de ce fait un facteur de transparence et a aussi permis de clarifier les droits et devoirs des personnes interrogées lorsqu'elles fournissent des renseignements à des fins statistiques.
Par ailleurs, la nouvelle loi contient un chapitre sur la protection et la sécurité des données. Mentionnons également que d'après les nouvelles dispositions, les données relevées à des fins statistiques peuvent être utilisées *exclusivement à des fins statistiques. Elles ne peuvent être exploitées à d'autres fins administratives que* si cela est expressément prévu dans une loi fédérale ou lorsque la personne concernée a donné son *consentement écrit*.

4.2. Révision de l'ordonnance sur le Registre des entreprises et des établissements (REE)

Du fait de son exhaustivité, ce registre sert depuis longtemps à d'autres fins que la statistique fédérale. Certains services fédéraux et cantonaux peuvent en effet utiliser une catégorie bien précise de données REE pour des tâches administratives. Il s'imposait donc de donner une base légale à l'utilisation des données du système à des fins non statistiques, voire administratives. Cette utilisation des données REE est désormais réglementée à l'article 10, 3e alinéa, LSF.

Le registre REE a été constitué en 1975 à la suite du recensement des entreprises et établissements. Il contient les noms et adresses, ainsi que d'autres indications importantes - telles que le nombre d'employés, la forme juridique, la date de l'inscription au registre du commerce, et le capital social des sociétés anonymes - de tous les établissements et entreprises enregistrés en Suisse. L'ordonnance révisée énumère de manière exhaustive les données figurant actuellement au Registre.
A l'origine, le registre REE servait de base d'adresses pour le recensement des entreprises et d'autres relevés statistiques fédéraux. Sa première base légale fut l'ordonnance du 12 décembre 1988 sur la tenue d'un registre des entreprises et établissements. La validité de cette base légale était néanmoins limitée à la fin de l'année 1993. Sa révision s'imposait donc.
Cette révision était également nécessaire du fait qu'en raison de son exhaustivité, le Registre. servait depuis longtemps à des fins autres que celles de la statistique fédérale. D'autres services fédéraux et cantonaux peuvent utiliser une catégorie bien précise de données REE *pour des tâches administratives*. Conformément à l'article 14 LSF, les données relevées à des fins statistiques ne peuvent être utilisées à d'autres fins que si une loi fédérale autorise expressément une autre utilisation ou si la personne concernée y a consenti par écrit.
Il fallait donc donner une base juridique à l'utilisation des données REE à des fins non statistiques ou à des fins administratives, ce qui fut fait à l'article 10, 3e alinéa LSF. En outre, l'ordonnance révisée du Registre REE a été adaptée aux exigences de la nouvelle LSF et de la nouvelle LPD. Les principales modifications effectuées sur la base de nos propositions sont les suivantes:

- les sources ainsi que le contenu du REE ont été redéfinis;
- l'utilisation des données a été réglementée dans les détails:
- la saisie, la mutation et l'archivage des données sont définis par de nouvelles dispositions;
- les liaisons avec d'autres systèmes d'information et les accès aux données sont énumérés de manière exhaustive en annexe à l'ordonnance.

4.3. Le recensement de la population de 1990

L'exploitation statistique des documents d'enquête est achevée depuis quelque temps. Ainsi que le prévoit l'article 25 de l'ordonnance du 26 octobre 1988 sur le rencensement fédéral de la population de 1990, il a fallu détruire ces documents conformément aux principes de protection des données. Nous avons à ce propos visité l'installation de destruction choisie par l'Office fédéral de la statistique à Berne pour nous faire une idée des mesures de sécurité retenues pour assurer une destruction des documents conforme à la protection des données.

Le dernier recensement fédéral de la population a été effectué en 1990. Une fois terminée l'exploitation statistique des documents d'enquête, qui contenaient également des données sensibles, il a fallu les détruire conformément aux principes de la protection des données, comme prévu à l'article 25 de l'ordonnance du 26 octobre 1988 sur le recensement fédéral de la population.
Tout d'abord, les questionnaires individuels du recensement de 1990 saisis de manière automatisée sur mandat de l'Office fédéral de la statistique auprès de l'Office fédéral de l'informatique ont été définitivement effacés le 14 mai 1993. Il a ensuite fallu détruire conformément aux principes de protection des données les informations personnelles encore disponibles sur papier (notamment les enveloppes pour les ménages privés, questionnaires individuels, documents auxiliaires,

bordereaux de bâtiments). Comme prévu, les services cantonaux avaient remis les documents d'enquête à l'Office fédéral de la statistique pour que celui-ci centralise leur élimination.
Nous avons ensuite visité l'installation de destruction des documents choisie par l'Office fédéral de la statistique afin de nous assurer des mesures de sécurité accompagnant l'élimination conforme aux principes de protection des données des documents d'enquête.
Cette destruction s'est déroulée de manière efficace et sans difficulté jusqu'au 2 novembre 1993. Quant aux bordereaux de bâtiments, ils seront vraisemblablement détruits au milieu de cette année.

4.4. Recensement de la population de l'an 2000

Pour que l'Office fédéral de la statistique puisse relever indirectement les données nécessaires au prochain recensement de la population prévu pour l'an 2000, il faut que les fichiers des cantons et des communes se substituent entièrement ou partiellement aux relevés directs. Certes la Confédération ne dispose pas de compétence constitutionnelle pour édicter de nouvelles dispositions fédérales sur la tenue de registres communaux et cantonaux. Un relevé indirect des données du recensement de la population doit néanmoins respecter les principes de la protection des données. Un relevé indirect, ou un recensement à partir de registres, doit donc s'accompagner de mesures qui garantissent la transparence du traitement des données. En outre, les mesures nécessaires doivent être prises pour que les données obtenues par le biais des registres cantonaux soient utilisées uniquement à des fins de recensement et non pour d'autres tâches administratives de la Confédération et des cantons.

Depuis l'entrée en vigueur de la nouvelle loi sur la statistique fédérale, il existe une seule exception au principe selon lequel certaines statistiques doivent être réglementées par voie d'ordonnance. Cette exception porte sur le recensement de la population. La loi du 3 février 1860 sur le recensement de la population, révisée en 1988, prévoit une périodicité de 10 ans et contient des dispositions sur l'année d'exécution, la répartition des tâches et des coûts entre Confédération et cantons, ainsi que sur la protection des données. Outre ces régles spécifiques, le recensement de la population est également soumis aux dispositions de la LSF. Mais le législateur n'a pas voulu intégrer la loi sur le recensement de la population dans la nouvelle LSF.

Conformément à l'article 4 LSF, la Confédération doit, lorsqu'elle dispose des données requises, renoncer à effectuer des relevés spécifiques auprès de la population afin d'éviter aux personnes concernées des questionnaires réitérés.
Le relevé indirect constitue un second moyen permettant de décharger la population: les données sont alors collectées à partir de fichiers cantonaux ou communaux, ou auprès d'organes qui ne sont pas soumis à la LSF, mais qui exécutent du droit fédéral.
L'Office fédéral de la statistique désire relever en partie indirectement les données nécessaires au prochain recensement de la population prévu en l'an 2000. Il faudra donc que les fichiers des cantons et des communes remplacent entièrement ou partiellement les relevés directs. Mais le relevé indirect des données nécessaires au recensement de la population requiert une modification des dispositions sur la tenue des registres du contrôle de l'habitant et des autres registres cantonaux afin de

permettre une utilisation adéquate de ces données à des fins statistiques. En outre, afin de rationaliser la reprise des données, il conviendrait d'édicter de nouvelles dispositions légales sur la liaison automatisée de ces registres. En d'autres termes, il faudrait édicter *de nouvelles dispositions fédérales* sur la tenue des registres communaux et cantonaux pour harmoniser ces registres.
La tenue des registres mentionnés plus haut relève néanmoins de la compétence des cantons, des communes et de leurs organes. Les organes de la Confédération ne peuvent intervenir dans le domaine législatif souverain des cantons que si la Constitution prévoit expressément une telle compétence. Or cette base constitutionnelle manque, et il faudrait la créer par une modification de la Constitution.

Mentionnons enfin qu'un relevé indirect des données du recensement de la population doit respecter les principes généraux de la protection des données, notamment celui de la proportionnalité. Bien que la nécessité et l'opportunité des relevés indirects soient incontestées, le traitement de données personnelles lors d'un recensement de la population doit être transparent. En effet, le relevé indirect de données permet de supprimer les barrières traditionnelles à l'information, qui permettent à chaque citoyen et citoyenne de déterminer eux-mêmes sous quel jour ils désirent se présenter aux autorités et de contrôler les données relevées, pour éventuellement rectifier les indications inexactes. Avec un relevé direct, le danger de traiter des données inexactes à l'insu des personnes concernées est moindre.
Pour cette raison, un relevé indirect ou un recensement au moyen de registres doit être accompagné de mesures propres à garantir la transparence du traitement des données. Une de ces mesures est l'information préalable des personnes concernées sur le traitement de données envisagé.
Il convient par ailleurs de relever que l'interconnexion à des registres cantonaux ne doit pas permettre le traitement des données à d'autres fins (détournement de finalité) que celles pour lesquelles elles ont été collectées (statistiques, recensement de la population). Il faut donc prendre les mesures requises pour que les données obtenues par le biais de registres cantonaux ne soient utilisées qu'à des fins de recensement et *non pas pour d'autres tâches administratives de la Confédération ou des cantons.*

Pour ces motifs, les données relevées par l'interconnexion de divers registres doivent être communiquées aux personnes concernées pour qu'elles soient informées des indications les concernant tout comme pour un relevé direct. Ce n'est que lorsque les citoyens et citoyennes connaissent les données traitées à leur propos qu'ils peuvent faire usage des droits garantis par la loi sur la protection des données (droits d'accès et de rectification des données notamment).

5. Santé

Les données relatives à la santé sont soumises à une protection juridique renforcée, en particulier lorsqu'elles sont traitées par des organes fédéraux. Voici à titre d'exemples deux questions pour lesquelles nous avons été consultés: l'ordonnance sur les études VIH et la mise en place d'un programme de distribution de drogue sous surveillance dans le cadre de l'évaluation de projets visant notamment à prévenir la toxicomanie. Information (transparence), consentement des personnes concernées, respect de leur volonté et anonymisation des données dès que possible sont

quelques uns des piliers de la protection des données. Le respect de ces règles est en outre générateur de confiance, élément indispensable au bon déroulement de toute étude entreprise dans le domaine de la santé.

Les données relatives à la santé sont considérées comme sensibles par la loi fédérale sur la protection des données (LPD). Le législateur les a de ce fait soumises à une protection juridique accrue. Les deux domaines évoqués ci-dessous nous ont été soumis pour avis. Les études sur le SIDA sont en cours, celles impliquant la distribution de drogue sous surveillance étant encore sous forme de projet.

SIDA
cette maladie est un sujet sensible par excellence, surtout de par les peurs irraisonnées qu'elle génère dans la population. Les employeurs et assureurs peuvent également être amenés à prendre des mesures préjudiciables pour les personnes porteuses du virus ou malades. De ce fait, lorsque l'Office fédéral de la santé publique nous a fait part de son projet d'effectuer dans notre pays des études sur la prévalence et l'incidence du virus de l'immunodéficience humaine (VIH), nous avons conseillé la plus grande prudence en la matière. Notre collaboration a abouti par l'adoption d'une ordonnance du Conseil fédéral, entrée en vigueur le 1er août 1993:
"l'ordonnance du 30 juin 1993 sur des études épidémiologiques visant à collecter des données sur le virus de l'immunodéficience humaine (ordonnance sur les études VIH)".

L'ordonnance prévoit notamment, *pour les études anonyme*s, l'obligation, pour les centres de prélèvement des échantillons, d'informer les participants d'une manière claire et compréhensible. Si le donneur ne déclare pas s'opposer à la recherche des anticorps anti-VIH dans son échantillon, son consentement est présumé. En cas de refus de participer, la volonté du donneur doit être respectée. Une obligation générale d'information du public est également prévue lorsqu'une étude anonyme est planifiée. Des échantillons ne peuvent en outre pas être prélevés aux seules fins d'étude VIH anonyme. Finalement, les échantillons doivent être anonymisés dans les centres de prélèvement, et ce n'est que sous cette forme qu'ils peuvent être expédiés aux centres de tests.

Pour les études avec le concours de volontaires (nominatives), l'information et le consentement des personnes testées sont également requis. L'attention de ces dernières doit être au demeurant attirée sur le fait qu'elles peuvent refuser leur consentement ou le retirer en tout temps. Les données collectées ne transitent pas par les centres de tests mais sont directement expédiées à l'organe central de l'étude. Le rapport d'étude est rédigé de manière à ce que les participants ne puissent pas être identifiés. Finalement, l'ordonnance prévoit des normes relatives à l'obligation de garder le secret, à la conservation des données et au droit d'accès, ainsi que la possibilité, pour les personnes sujets de tests, de requérir la médiation du Préposé aux études.

Ces mécanismes destinés à assurer une protection optimale de la personnalité des participants à des études VIH, visent également, surtout par le biais de la transparence (information) et d'une certaine liberté de décision (consentement des donneurs) à générer la confiance au sein de la population, respectivement des "groupes à risques".

Distribution de drogue sous surveillance: une ordonnance du Conseil fédéral entrée en vigueur le 15 novembre 1992, avec effet jusqu'au 31 décembre 1996, fixe le cadre dans lequel une évaluation de mesures propres à prévenir la toxicomanie, à améliorer l'état de santé des personnes dépendantes et leurs conditions de vie, à les réinsérer dans la société, ainsi qu'à réduire la délinquance liée à l'acquisition de stupéfiants peut être entreprise: *"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".*

A cette fin, des essais sur des groupes comptant 50 toxicomanes par essai sont prévus, sous la surveillance de l'Office fédéral de la santé publique. Dans ce contexte des stupéfiants seront distribués sous contrôle, à savoir, héroïne, morphine, ou méthadone. Un plan global d'étude contenant également des dispositions d'exécution est en cours d'élaboration, ainsi que, notamment, un projet de "déclaration de consentement" que chaque participant à un essai devra signer. L'Office fédéral de la santé publique nous a soumis ces deux documents pour avis en janvier 1994.

Nous avons recommandé à cet organe de tout mettre en oeuvre pour que cette évaluation se déroule dans un climat de confiance, condition sine qua non pour obtenir de bons résultats. A cette fin, nous avons mis l'accent sur les points suivants:

- soumission à la LPD de tous les traitements de données personnelles effectués dans le cadre de l'évaluation, indépendamment de l'organe qui procèdera aux traitements;

- devoir des responsables des essais de veiller à ce que le consentement des participants aux tests soit aussi libre et éclairé que le permet l'état de toxicodépendance de ces personnes;

- consentement limité dans le temps et spécifique quant à son objet. Afin de garantir cette spécificité, le formulaire de "déclaration de consentement" est à libeller de manière à ce que la personne concernée ne soit pas tenue de donner un consentement global, mais puisse diversifier ses réponses, selon qu'on lui demande par exemple son accord pour se soumettre à un test HIV, pour qu'un extrait de son casier judiciaire soit demandé en début, puis en fin d'essai, ou pour que des médecins ou des auxiliaires soient déliés du secret médical;

- devoir des organes responsables de l'enquête d'empêcher toute communication de données relatives aux participants à des tiers, en particulier à des autorités administratives ou de police, et ce indépendamment du consentement des personnes concernées. D'une part, les principes généraux de protection des données s'y opposent (principes de proportionnalité et de finalité), et d'autre part, le bon déroulement de l'évaluation pourrait pâtir d'une telle communication.

Nous avons pour ces motifs conseillé à l'Office fédéral de la santé publique de réviser le plan global et le formulaire de "déclaration de consentement" en conséquence.

6. Génétique

Suite à l'entrée en vigueur de l'article 24novies de la constitution fédérale (cst), nous avons été appelés à nous prononcer sur l'admissibilité, en l'état actuel du droit, du recours à l'analyse ADN (méthode Jeffrey) en matière d'établissement ou d'exclusion de la paternité. Nous avons considéré que la méthode Jeffrey était actuellement la plus appropriée, obéissant aux principes généraux de protection des données, en particulier ceux de proportionnalité et d'exactitude.
Quant au traitement des échantillons requis en particulier pour la recherche sur l'homme, nous avons exprimé l'avis qu'il requiert, en raison des caractéristiques propres auxdits échantillons, l'élaboration de normes spécifiques de protection des données. Afin que ces normes soient satisfaisantes pour tous, nous avons finalement souligné l'importance, pour nos services, d'être associés aux travaux de réflexion actuellement en cours.

Le 17 mai 1992 entrait en vigueur l'article 24novies de la constitution fédérale (cst) relatif à la génétique et à la procréation assistée. Cette disposition vise à protéger l'homme et son environnement contre les abus en matière de techniques de procréation et de génie génétique, et fonde notamment la compétence de la Confédération pour édicter des prescriptions visant à assurer la protection de la personnalité. Cette norme prévoit en outre que "le patrimoine génétique d'une personne ne peut être analysé, enregistré et révélé qu'avec le consentement de celle-ci ou sur la base d'une prescription légale". Dès l'automne 1992, l'Office fédéral de la justice commençait les travaux de prospection. Cet organe nous a contactés en nous priant notamment de nous prononcer sur la légitimité de lege lata de l'usage de l'analyse de l'empreinte génétique (analyse ADN) en matière de recherche en paternité, et sur les incidences de l'article 24novies cst sur les principes juridiques de recherche existants. Nous nous sommes exprimés en ces termes:

Analyse ADN et recherche en paternité: alors que l'analyse du sang apportait de nombreuses informations autres que celles nécessaires à l'exclusion ou à l'établissement d'une paternité, la méthode dite "Jeffrey" est moins "parlante". En effet, en matière de recherche en paternité, il n'est pas nécessaire d'analyser les 5% d'ADN qui contiennent des séquences codantes (Erbfaktoren), mais il suffit de travailler sur les parties "non codantes" d'ADN situées à des endroits précis des chromosomes. Grâce aux différences de longueurs existant entre ces segments (polymorphies de longueurs), l'individualisation est possible. Il semble en outre que cette méthode, en matière d'exclusion de paternité, soit sûre à 100%. En matière d'établissement positif de la paternité, le degré de fiabilité est en outre supérieur aux 99,8% requis par le Tribunal fédéral. Nous avons donc conclu que, considérée à la lumière des principes généraux de protection des données, en particulier des principes de proportionnalité et d'exactitude, la méthode Jeffrey était le mode d'analyse à ce jour le plus approprié.

Article 24novies cst et recherche sur l'homme: l'article 321bis du code pénal (CP) entrait en vigueur simultanément à la LPD, permettant notamment la constitution d'une "Commission d'experts du secret professionnel en matière de recherche médicale" (ci-après la commission), entrée en fonction en janvier 1994. Si les conditions de cette disposition pénale sont remplies, la commission est compétente pour décider de l'octroi ou non d'une autorisation de communiquer des données personnelles à des fins de recherche dans les domaines de la médecine ou de la santé publique. Nous avons émis l'avis que, bien qu'applicable aussi bien aux

secteurs privé que public, tant cantonal que fédéral, l'article 321bis CP ne suffisait pas à couvrir tous les cas de recherche dont il est question à l'article 24novies cst. D'autre part, nous avons rappelé que le champ d'application des règles de protection des données ne pouvait pas être étendu sans autre aux échantillons prélevés à des fins de recherche génétique, exception faite des normes régissant la collecte des données. En effet, outre le fait qu'un échantillon constitue en quelque sorte une source d'informations infinie sur laquelle l'individu ne peut pratiquement plus avoir de maîtrise, il est susceptible de livrer non seulement des informations sur la personne concernée, mais également sur sa lignée, tant ascendante que descendante. Il est de ce fait nécessaire d'édicter des normes spécifiques de traitement des échantillons, y compris leur conservation, leur transmission et leur destruction, ce que l'article 24novies cst permet pour les échantillons prélevés à des fins de recherche génétique. Nous avons finalement attiré l'attention de l'Office fédéral de la justice, ainsi que du Département fédéral de l'intérieur sur la nécessité de nous associer aux travaux de tout groupe d'étude constitué sur la base de l'article 24novies cst, dans la mesure où des données personnelles ou des échantillons humains sont concernés. Ce n'est qu'ainsi que les exigences de la protection des données pourront être intégrées de manière harmonieuse dans de nouvelles normes régissant la génétique et la procréation assistée.
Nous ne sommes pour l'instant qu'au début de nos investigations relatives aux problèmes de protection des données soulevés par la génétique, dans des domaines aussi variés que la recherche, les assurances sociales ou privées ou le droit du travail. Avant d'intervenir dans un domaine aussi délicat, il convient cependant d'être circonspects. Nous ne pouvons dès lors que répéter que des solutions à la fois praticables et aptes à garantir les droits de la personnalité ne pourront être trouvées que si nous sommes dès le début associés aux travaux de réflexion entrepris dans ces domaines.

7. Assurances

7.1. Assurances sociales

A l'instar du secteur de la santé, le domaine des assurances requiert le traitement de données sensibles et de profils de la personnalité. Pour ce type de données, des normes de protection accrues ont été introduites dans la LPD, comme le demandait le "rapport Jaggi" de 1984. Dans le domaine des assurances sociales, de nombreuses lacunes doivent encore être comblées, la problématique des flux d'informations médicales, notamment à destination des caisses-maladie, n'étant à ce jour pas réglée (cf. à titre d'exemple, la nouvelle liste des analyses et tarif, entrée en vigueur le 1er janvier 1994). Contrairement aux assurances sociales, dotées la plupart du temps de normes matérielles spécifiques de protection des données, le secteur des assurances privées est entièrement régi par les normes de la LPD applicables au secteur privé. Depuis l'entrée en vigueur de la loi, nous avons établi les premiers contacts avec l'une ou l'autre compagnie d'assurance, particulièrement pour ce qui relève du devoir d'annonce de fichiers. Au niveau européen, le Conseil de l'Europe a mis sur pied un groupe de travail auquel nous participons, chargé d'élaborer un projet de recommandation relative à la protection des données à caractère personnel collectées et traitées à des fins d'assurance privée.

En février 1984 déjà, le rapport d'une commission instituée par l'Office fédéral de la justice, intitulé "protection des données dans le domaine médical" (rapport Jaggi) a brossé un tableau plutôt sombre de la problématique du traitement (en particulier la communication) de données médicales, notamment en matière d'assurances sociales et privées. Le rapport concluait entre autres à la nécessité de soumettre ces données à une protection accrue, ce qui a été fait dans la LPD.
D'une part, les activités des assurances sociales sont en principe régies par des normes matérielles spécifiques de protection des données. D'autre part, lorsque la LPD s'applique, elle pose un certain nombre de problèmes aux caisses de pension et aux caisses professionnelles en particulier, telle la question de l'annonce des fichiers au préposé. Nous vous faisons part dans le point suivant de la réponse que nous avons apportée à cette problématique. Vient ensuite la nouvelle "liste des analyses et tarif", ordonnance du Département fédéral de l'intérieur entrée en vigueur le 1er janvier 1994, qui illustre le fait que la plupart des manquements à la protection des données signalés dans le rapport Jaggi sont toujours actuels, en particulier le problème des flux d'informations médicales. Quelques considérations relatives aux assurances privées bouclent ce bref tour d'horizon.

Droit de la protection des données applicable aux caisses de compensation cantonales et aux caisses professionnelles, en particulier sous l'angle du devoir d'annonce.

Afin de lever le doute auprès des caisses de compensation cantonales et des caisses professionnelles en matière d'annonce de fichiers, nous leur avons adressé les précisions suivantes:
Si une caisse de compensation gère des fichiers de données personnelles en application du droit cantonal, par exemple en matière de compensation familiale, elle annonce ces fichiers aux autorités cantonales de protection des données dans les cantons dotés d'une telle loi.
Lorsqu'une telle caisse exécute du droit fédéral (AVS par exemple), elle déclare les fichiers tenus à cette fin aux autorités cantonales de protection des données, dans les cantons dotés d'une loi sur la protection des données. Dans les cantons qui ne disposent pas encore d'une telle loi, l'annonce est faite auprès de l'organe de contrôle cantonal que ces cantons sont tenus de désigner selon la LPD.
Quant à la caisse professionnelle qui agit en tant que personne privée (fonds de vacances), elle est uniquement soumise au devoir d'annonce dans les cas prévus par la LPD. Pour les fichiers qu'elle gère en tant qu'organe fédéral (prévoyance professionnelle obligatoire, LPP), elle est toujours soumise au devoir d'annonce, comme tous les organes fédéraux.

Nouvelle liste des analyses et tarif (ci-après la liste)

L'existence de la liste a été portée à notre connaissance par la FMH et la "Schweizerische Patienten Organisation" (SPO). Ces deux organisations ont attiré notre attention sur les nouveaux problèmes de protection des données que l'entrée en vigueur de la liste révisée risquait de provoquer.

Le texte de la liste n'étant pas en notre possession et le fonctionnement de cet instrument à l'usage des laboratoires d'analyses ne nous étant pas connu, nous avons émis, le 15 décembre 1993, *une recommandation* à l'adresse de l'Office fédéral des assurances sociales, afin qu'il diffère la date d'entrée en vigueur de la

liste, jusqu'à ce que nous ayons pu l'examiner sous l'angle de la protection des données. Vu l'urgence de la situation, nous avons, le 20 décembre 1993, déposé *une demande de mesures provisionnelles* auprès du Président de la Commission fédérale de la protection des données, le priant de repousser la date d'entrée en vigueur de la liste. Le 23 décembre 1993, nous avons été invités par le Secrétaire général du Département fédéral de l'intérieur. Des représentants de l'Office fédéral des assurances sociales ont assuré qu'il était techniquement difficilement réalisable de retarder l'entrée en vigueur de la liste, tous les laboratoires d'analyses ayant déjà procédé à l'adaptation de leurs systèmes informatiques (information qui s'est par la suite avérée inexacte pour la plupart des laboratoires privés). L'existence de problèmes de protection des données a en outre été reconnue, et mandat a été donné à l'Office fédéral des assurances sociales de constituer un groupe de travail. Ce dernier devra dans un premier temps réviser la liste et l'adapter aux exigences de la protection des données, l'examen de la problématique globale des flux d'informations à destination des caisses d'assurance constituant la deuxième partie de sa tâche. Le 24 décembre 1993, des laboratoires d'analyses privés, soutenus par des laboratoires publics, ont déposé *un recours*, respectivement *une dénonciation* au Conseil fédéral, demandant à titre provisionnel la suspension de la mise en vigueur de la liste. L'issue de cette procédure ne nous est à ce jour pas connue. Le 17 janvier 1994, le Président de la Commission fédérale de la protection des données rejetait les recours déposés par la FMH et la SPO (en l'absence de décision formelle du Département fédéral de l'intérieur), déniant la qualité pour recourir à la FMH et considérant notamment que la SPO n'avait pas apporté d'éléments suffisants susceptibles de justifier la suspension de la liste. Le 25 janvier 1994, nous nous sommes prononcés sur un projet de décision de constitution du groupe de travail susmentionné. Nous sommes depuis lors dans l'attente d'une nouvelle proposition. Le 23 février 1994, le Préposé à la protection des données du canton de Berne nous soumettait à son tour la problématique de la nouvelle liste.

Quelques problèmes posés par la liste: sur la base des informations qui nous ont été livrées par les divers intervenants, nous avons constaté que la nouvelle liste pose, tant du point de vue de la protection des données que du secret médical, de nouvelles difficultés dont nous signalons ici les plus évidentes:

- la nouvelle liste implique l'indication du prélèvement analysé et du résultat de l'analyse sur la facture;
- la nouvelle liste affine le détail de la facturation pour des tests aussi délicats que ceux du SIDA, de l'hépatite b ou de tumeurs cancéreuses;
- le destinataire de la facture est informé du résultat positif ou négatif d'une analyse, le nombre de points facturés dépendant du résultat.

Dès lors, les médecins ne sont plus en mesure de garantir un minimum de respect du secret médical à leurs patients, et les laboratoires d'analyses tenus d'appliquer la nouvelle liste violent le devoir de discrétion ancré dans la LPD.
La communication d'informations aussi détaillées aux caisses-maladie est finalement problématique. Dans la plupart des caisses, les résultats d'analyses sont accessibles au personnel administratif. Le "filtre" du médecin-conseil fait défaut, ou, s'il s'agit d'une petite agence dotée d'un ou deux représentants qui connaissent personnellement les assurés, il y a des risques de "fuites" ou un cumul de fonctions pouvant être incompatibles entre elles.

7.2. Assurances privées

Ces dernières années, un vent de déréglementation souffle dans le domaine des assurances privées en Suisse, et ce afin de rendre la législation en la matière eurocompatible.
Cet assouplissement de la surveillance de l'Etat n'a cependant pas d'incidence directe sur la protection de la personnalité des assurés, le secteur des assurances privées étant entièrement régi par la LPD, et ce depuis le 1er juillet 1993. Au niveau national, nous avons établi les premiers contacts avec l'une ou l'autre grande compagnie d'assurance dès l'entrée en vigueur de la LPD, particulièrement pour ce qui relève du devoir d'annonce de fichiers. Sur le plan européen, en février 1994, nous avons participé à la première réunion du groupe de travail 14, chargé de l'élaboration d'un projet de recommandation du Conseil de l'Europe relative à la protection des données à caractère personnel collectées et traitées à des fins d'assurance privée.

8. Archives

8.1. Nouvelle loi sur les archives

Suite aux événements survenus ces dernières années à l'échelle nationale et internationale, surtout européenne, il s'est avéré nécessaire d'édicter une nouvelle réglementation sur les archives, et ce sous forme de loi. Cette nécessité est essentiellement apparue suite aux problèmes que posaient l'application de l'obligation de verser aux archives des informations à caractère personnel, sensibles et enregistrées sur des supports électroniques de données. En outre, la LPD établit que le traitement de données sensibles ou de profils de la personnalité par des organes fédéraux doit reposer sur une loi au sens formel. Pour ces motifs, nous participons à l'élaboration d'une loi sur les Archives fédérales au sein d'un groupe de travail interdépartemental.

Les organes fédéraux doivent détruire les données personnelles dont ils n'ont plus besoin ou les rendre anonymes à moins qu'elles ne doivent être conservées à titre de preuve ou par mesure de sûreté, ou encore être déposées aux Archives fédérales.
Conformément au règlement du 15 juillet 1966 pour les Archives fédérales, actuellement encore en vigueur, les membres, fonctionnaires et employés de l'Assemblée fédérale et de ses commissions, du Conseil fédéral ainsi que des services et des établissements de l'administration générale de la Confédération, des commissions administratives, des commissions d'experts et d'autres commissions extraparlementaires, dont le secrétariat est assuré par l'administration générale de la Confédération, ainsi que des établissements fédéraux autonomes qui viennent à disparaître ou qui veulent se dessaisir d'actes importants sont tenus de verser aux Archives fédérales leurs documents officiels.

Par ailleurs, les Archives fédérales conservent des fonds pouvant servir à l'histoire de la Suisse depuis 1798, qu'il s'agisse de fonds déposés, donnés, légués ou acquis d'une autre manière, ainsi que diverses collections de copies, de photocopies, de microfilms, de registres et d'inventaires concernant l'histoire de la Suisse et provenant d'autres archives et bibliothèques.

Les Archives fédérales abritent par conséquent d'énormes quantités de données personnelles, de données sensibles et de profils de la personnalité.

Outre le besoin d'une nouvelle réglementation des activités des organes fédéraux en matière de consultation et de gestion des écrits et des informations de l'administration, ainsi que du devoir d'archivage et de dépôt, il est apparu nécessaire de réorganiser les archives surtout en raison des problèmes que posait l'obligation de déposer les informations à caractère personnel, sensibles et enregistrées sur supports électroniques. Par ailleurs, la LPD requiert que le traitement de données sensibles ou de profils de la personnalité par des organes fédéraux repose sur une loi au sens formel.

Un groupe de travail interdépartemental a été créé en 1993. Constitué de représentants de divers secteurs intéressés de l'administration fédérale, il a pour tâche d'élaborer un projet de loi sur les Archives fédérales. La protection des données y est également représentée.

De notre point de vue, cette loi doit avoir les objectifs suivants:
- pour des raisons de transparence, la création d'un texte légal uniforme, réglementant de manière approfondie le domaine des archives pour qu'on puisse si possible éviter les réglementations spécifiques dans des domaines extérieurs à la loi sur les Archives fédérales;
- pour des raisons de transparence et d'uniformité, une répartition claire des compétences en faveur des Archives fédérales suisses après le versement de documents à ces mêmes Archives pour qu'en cas de doute et de litige, il n'y ait qu'un seul interlocuteur chargé de prendre les décisions et qu'une certaine unité de doctrine soit ainsi garantie;
- pour des raisons de meilleure connaissance du secteur où les données ont été traitées à l'origine, l'établissement d'un devoir pour les Archives fédérales de consulter avant toute décision, en cas de doute et de litige, les services fédéraux qui ont versé les documents;
- pour des raisons de sécurité du droit enfin, la création de règles claires applicables au traitement de données sensibles (au sens large et selon la LPD) ainsi que de profils de la personnalité, notamment par la fixation de délais de protection en relation avec le droit de consulter des dossiers sensibles et/ou contenant des données sensibles (au sens de la LPD) et des profils de la personnalité.

8.2 "Les enfants de la grand-route"

L'activité de l'oeuvre d'entraide "Les enfants de la grand-route" a fortement préoccupé l'opinion publique dans les années 80. Par la suite, la question s'est posée de savoir dans quelle mesure il fallait autoriser les personnes concernées et les tiers (à des fins de recherche) à consulter la vaste documentation de cette oeuvre d'entraide. Bien que la plupart des dossiers ne tombent pas dans le champ d'application de la LPD, nous avons pris position sur les différentes questions de la réglementation de la consultation par les personnes concernées et par les tiers.

De 1926 à 1973, la fondation Pro Juventute a dirigé l'oeuvre d'entraide "Les enfants de la grand-route", dont le but était de lutter contre le "vagabondage" en séparant les enfants jenisch de leurs parents. C'est ainsi que 600 enfants ont été placés chez des

parents nourriciers, dans des homes pour enfants, des orphelinats, des cliniques psychiatriques et des maisons d'éducation. Cette oeuvre d'entraide a bénéficié du soutien, non seulement des autorités cantonales, mais aussi de la Confédération. Une quantité incroyable de données, en partie très délicates et particulièrement sensibles, ont été collectées. En 1973, l'oeuvre d'entraide a cessé ses activités. Dès 1985, des efforts ont été entrepris pour réparer le tort causé aux personnes concernées; ces efforts ont conduit à la création de deux commissions. La Commission des dossiers "Enfants de la grand-route" a examiné, avec l'aide des cantons concernés, si et dans quelle mesure il fallait autoriser les personnes concernées à consulter leurs dossiers. La Commission des fonds a traité de la question de l'indemnisation des personnes concernées. Dans le cadre de l'activité de la Commission des dossiers dissoute en 1993, quelque 240 personnes se sont vu accorder le droit de consulter leurs dossiers.

Afin d'établir les responsabilités et de réparer l'injustice dont elles ont été les victimes, les personnes concernées, auxquelles se sont jointes l'opinion publique, Pro Juventute et la Confédération, ont demandé une étude scientifique relative à ces événements. La question s'est alors posée de savoir dans quelle mesure les personnes concernées disposaient d'un droit d'être consultées au sujet de la mise sur pied de cette étude et - ceci est important pour le droit de la protection des données - si l'on pouvait consulter leurs dossiers à des fins de recherche, sans leur consentement.

Comme le pouvoir décisionnel concernant les dossiers appartient aux cantons, la LPD n'est en principe pas applicable. Nous avons toutefois été priés de prendre position sur la question de la consultation des dossiers à des fins de recherche, ainsi que sur une réglementation générale de la consultation par les personnes concernées, tant des dossiers de Pro Juventute que des nouveaux dossiers établis par les deux commissions susmentionnées.

Nous avons remis plusieurs prises de position sur ces questions complexes. Elles n'ont toutefois aucun caractère obligatoire dans la mesure où la LPD n'est pas applicable (à savoir pour les dossiers qui dépendent du pouvoir décisionnel des cantons).

En ce qui concerne la question la plus importante, c'est-à-dire la réglementation de la consultation des dossiers par les personnes concernées et à des fins de recherche, ainsi que l'application du droit de rectification des données inexactes, les éléments suivants sont apparus:

bien que les divers dossiers soient soumis au pouvoir décisionnel de différents organes, et ainsi à différentes normes juridiques, *une réglementation uniforme de la consultation des dossiers*, pour laquelle une seule autorité serait compétente, est souhaitable dans l'intérêt des personnes concernées. Malgré le souhait exprimé de part et d'autre, nous ne pouvons pas être cette autorité compétente, car cette nouvelle tâche pourrait être incompatible avec notre fonction de surveillance en matière de protection des données.
A notre avis, la réglementation de la consultation devrait s'aligner sur la réglementation du droit d'accès prévue dans la loi sur la protection des données. Elle devrait fixer dans le détail qui a le droit de consulter les dossiers, l'étendue de ce droit, et pour quels motifs il peut être limité dans des cas d'espèce.

Comme les personnes concernées ont souvent exigé un droit d'être consultées, voire une compétence décisionnelle s'agissant de *la consultation de leurs dossiers par des tiers* à des fins de recherche, on ne peut pas partir de l'idée de leur consentement tacite. Il faut donc obtenir leur accord exprès avant une consultation à des fins de recherche. Seule une réglementation expresse dans une loi au sens formel permettrait de passer outre. De même, il faut clarifier la question de l'octroi du droit de consultation des dossiers à des tiers à d'autres fins que la recherche. Un tel droit ne devrait être octroyé qu'à partir du moment où aucune des personnes concernées n'est encore en vie, donc susceptible d'être gênée par cette consultation. A ce sujet, le délai de blocage de 35 ans fixé à l'article 7 du règlement pour les archives fédérales n'est pas suffisant.

Parmi les personnes concernées, certaines ont demandé à plusieurs reprises la destruction des données inexactes contenues dans les dossiers; d'autres en ont simplement demandé *la rectification*. Selon la LPD, toute personne qui traite des données doit s'assurer de leur exactitude. Chaque personne concernée peut exiger la rectification d'une donnée inexacte. Le droit à la destruction des données erronées et à leur remplacement par des données exactes existe du simple fait qu'une fausse indication peut nuire à la personne concernée lors d'un traitement ultérieur. La remise des dossiers aux personnes concernées, demandée par certains intéressés, n'est pas prévue dans la LPD.

Abstraction faite de la destruction de tous les dossiers, qui irait à l'encontre des intérêts des personnes concernées s'agissant des éclaircissements de leur passé personnel, ainsi que de l'opinion publique dans l'analyse historique de l'oeuvre d'entraide "Les enfants de la grand-route", une destruction des données erronées n'entre pas en ligne de compte, déjà pour des raisons pratiques. En outre, il s'agit dans la plupart des cas de jugements de valeur négatifs (la personne concernée est jugée faible d'esprit, paresseuse, etc.). De tels qualificatifs sont bien entendu très douloureux pour la personne concernée et lui ont causé beaucoup de tort par le passé; mais à l'avenir, ils pourront tout au plus porter préjudice à l'intéressé si le responsable de ces travaux n'arrive pas à prendre toute la distance voulue à l'égard de ces jugements de valeur.

C'est pourquoi, en se référant à l'article 15, 2e alinéa, OLPD, qui prévoit la possibilité de faire ajouter aux données personnelles déposées aux Archives fédérales la mention de leur caractère litigieux ou inexact, il faudrait donner aux personnes concernées la possibilité d'apporter une rectification dans leurs dossiers, qui attirerait l'attention sur la non-validité de ces jugements de valeur. Dans ce contexte, il est tout aussi important, lors d'un futur travail de recherche, d'exiger expressément la réfutation de tels jugements et la présentation objective des tenants et aboutissants.

A notre avis, il serait préférable de régler dans une loi au sens formel ces questions complexes relatives aux dossiers de l'oeuvre d'entraide "Les enfants de la grand-route", afin d'être sûr de trouver une réglementation qui préserve les intérêts des personnes concernées, tout en leur permettant d'influer dans un acte législatif sur le respect de leurs intérêts.

9. Personnel

9.1. Secteur privé

Les rapports de travail donnent lieu à un traitement souvent très complet et parfois long de données personnelles relatives aux travailleurs par l'employeur. Etant donné la dépendance en fait et en droit du travailleur vis-à-vis de l'employeur, il convient d'accorder une attention particulière à la protection des données et de veiller à ce que le traitement, par l'employeur, de données concernant les employés ne porte pas atteinte à la personnalité de ceux-ci. Le nouvel article 328b du code des obligations (CO) définit le contrôle, du point de vue de la protection des données, du traitement des dossiers de candidature et des dossiers du personnel, de la communication de données à des tiers et du droit de rectification pour les travailleurs lorsque qualifications et certificats contiennent des données inexactes.

Chaque firme possédant des employés traite des données personnelles. Il n'est donc pas étonnant que la protection des données dans les rapports de travail soit un aspect majeur de la problématique du traitement des données pas des personnes privées. Quelque dix rapports ont été rédigés à ce sujet depuis l'entrée en vigueur de la LPD. Les réponses aux questions les plus fréquentes ont été résumées dans des fiches techniques, remises ensuite à de nombreuses personnes intéressées. Par ailleurs, énormément de renseignements ont été fournis par téléphone.

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 est une norme spéciale établissant, dans le domaine de la législation sur le contrat de travail, une disposition de protection des données spécifique à propos du traitement, par l'employeur, de données personnelles concernant le travailleur. Cette norme a été introduite à la fois parce que les rapports de travail donnent lieu à un traitement d'informations relatives au travailleur souvent très complet et de longue durée, et que l'intéressé dépend en fait et en droit de son employeur, dépendance qui requiert une protection renforcée. L'article 328b CO a le pas sur la LPD et sur 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 du traitement des données, notamment le principe de la proportionnalité. En effet, il prévoit que l'employeur est autorisé à traiter des données relatives aux travailleurs dans deux cas seulement et uniquement dans une mesure précise: dans le cadre de la conclusion d'un contrat de travail, il est autorisé à traiter des données concernant les candidats afin de déterminer s'ils sont aptes à remplir l'emploi en question; par ailleurs, durant les rapports de travail, il peut traiter les données nécessaires à l'exécution du contrat de travail.

Outre l'article 328b CO et les principes généraux de traitement, il convient de noter essentiellement, à propos du traitement de données personnelles dans les rapports de travail, les principes régissant le traitement des données par des personnes privées et les motifs justificatifs d'une atteinte à la personnalité.

Nous allons aborder ci-dessous, dans l'ordre chronologique de déroulement des rapports de travail, les questions les plus importantes que nous avons traitées jusqu'ici.

Procédure d'engagement

Les problèmes relatifs à la protection des données surgissent dès la *publication d'une offre d'emploi*. Il arrive qu'une telle offre soit publiée sous chiffre, sans indication de l'employeur ou de l'entreprise de recrutement de personnel. Or si les candidats ne connaissent pas l'identité de l'annonceur, ils ne peuvent faire valoir leur droit d'accès. Ce qui peut s'avérer déplaisant lorsque par exemple des candidats dont le dossier a été rejeté désirent savoir si leur dossier de candidature est conservé. Le maître d'un fichier qui charge un tiers de traiter des données demeure tenu de fournir les renseignements demandés. Cette obligation incombe toutefois au tiers s'il ne révèle pas l'identité du maître du fichier. Ni l'éditeur du journal, ni l'entreprise qui publie l'annonce ne peuvent donner de renseignements complets sur une annonce sous chiffre car ils ne disposent généralement que du texte de l'annonce et transmettent ensuite directement les réponses qui leur parviennent. Ils doivent donc révéler à la candidate ou au candidat qui le demande l'identité de l'annonceur pour qu'elle ou lui puisse exercer son droit d'accès.

Pour ce qui est des candidatures, l'employeur ne peut que demander des documents ou poser *les questions qui se rapportent aux qualités requises par l'emploi* en question et dont il a besoin pour déterminer si la candidate ou le candidat est apte à le remplir.

Il en va de même de la recherche de *renseignements auprès de tiers* sur les candidats. A ce propos, il est en outre nécessaire que la personne concernée donne son accord. Par exemple on ne peut demander de renseignements auprès de l'employeur précédent que si la candidate ou le candidat a donné son accord. En principe, le travailleur possède un droit à l'autodétermination sur ses données. Ce droit figure déjà à l'article 330a CO, selon lequel l'employé peut lui-même décider s'il désire un certificat de travail complet ou une simple attestation de la part de l'employeur. Il en découle au moins implicitement un devoir de discrétion de la part de l'employeur. Le message concernant la loi fédérale sur la protection des données va également dans ce sens. Le droit donné par la loi au travailleur de limiter le flux d'informations le concernant ne doit pas être détourné dans son dos.

Même lorsque le travailleur a donné son accord à la communication de renseignements, ceux-ci doivent *se limiter aux informations essentielles concernant l'activité en question*. Il ne doit porter que sur les prestations et le comportement du travailleur durant les rapports de travail. Il est notamment illicite de garantir l'accès au dossier du travailleur, ou de communiquer les conditions du contrat de travail, car la position du candidat pourrait s'en trouver de ce fait considérablement affaiblie. Le nouvel employeur potentiel n'est évidemment pas en droit de recueillir sur le travailleur des renseignements que selon la loi, il ne pourrait pas obtenir de ce dernier personnellement.

L'analyse graphologique de l'écriture d'un candidat n'est également autorisée qu'avec l'accord exprès de celui-ci. Ce genre d'analyse répond en général à la

définition du profil de la personnalité (assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique) et contient souvent des indications révélatrices sur la personne en question. L'usage qui consiste à demander à tous les candidates et canditats une lettre de candidature manuscrite pour le cas échéant faire établir une analyse graphologique n'est pas conforme aux exigences de la loi sur la protection des données.

Il ressort en outre de l'article 328b CO et du principe de la proportionnalité que les dossiers des candidats qui n'ont pas été retenus doivent leur être retournés et que les éventuelles copies doivent être détruites immédiatement après conclusion de la procédure d'engagement.

Durant les rapports de travail

Durant les rapports de travail, un dossier du personnel concernant le travailleur est en général tenu. Conformément à l'article 328 CO, ces dossiers ne doivent contenir que les données nécessaires à l'exécution du contrat de travail.

Ces dossiers ne font l'objet d'un devoir de déclaration auprès de notre Secrétariat que dans certaines conditions. S'ils ne contiennent que des données dont le traitement par l'employeur est soumis à une obligation légale, si la personne concernée en a connaissance ou s'il n'y a pas de traitement régulier de données sensibles ou de profils de la personnalité, ni communication régulière de données à des tiers, ces fichiers ne sont pas soumis au devoir d'annonce.

Dans le contexte de *la qualification* des travailleurs (mais aussi de l'établissement de certificats intermédiaires et de certificats de départ) ainsi que de la communication de renseignements au nouvel employeur, se pose la question de savoir si les opinions sur le travailleur constituent des données personnelles et s'il existe un droit à la rectification (article 5, 2e alinéa, LPD) de ces opinions. Dans la mesure où elles sont ou peuvent être mises en relation avec une personne identifiée ou identifiable, les opinions constituent des données personnelles. Ces opinions doivent être contrôlées quant à leur exactitude et si nécessaire rectifiées. Il convient de distinguer trois cas :

- les appréciations purement subjectives (ex. "cette personne ne m'est pas sympathique", etc). Il est impossible d'en contrôler l'exactitude. Néanmoins, elles n'ont que faire dans un dossier du personnel car elles ne sont pas utiles à l'estimation de la personne en question;

- les appréciations subjectives qui reposent sur des critères objectifs (ex. "l'employé ne remplit pas la tâche requise, est paresseux, on ne peut pas compter sur lui, il fait bien son travail", etc.). Ici, l'appréciation est certes subjective, mais on peut examiner si elle repose sur des critères objectifs et est vérifiable par des tiers. Si oui, elle doit être considérée comme juste. Sinon, il convient de la rectifier;

- les appréciations dont on ne peut pas toujours démontrer l'exactitude ou l'inexactitude (par ex. "pourrait être plus productif"). Par analogie avec l'article 15, 2e alinéa, LPD, il convient dans ce cas d'apporter la mention de leur

caractère litigieux. Une meilleure solution, bien que non prévue par la loi, consiste à intégrer au dossier de la personne concernée sa propre "réponse".

La question se pose également de savoir si et dans quelle mesure les travailleurs ont *le droit d'accès* aux documents contenus dans leur dossier ou même le *droit de consulter* ces documents.

Il ressort de l'article 8 LPD que toute personne employée dispose d'un *droit d'accès complet au contenu de son dossier*. Ce droit d'accès ne peut être limité qu'exceptionnellement et dans des cas fondés. Il n'est notamment pas admis de limiter systématiquement la consultation des qualifications. Les dossiers du personnel doivent être tenus de manière à ce que l'on puisse renseigner les travailleurs sur tout et à ce que le droit d'accès ne soit qu'exceptionnellement limité, et uniquement en raison de circonstances extraordinaires. Par ailleurs, il est permis de restreindre ce droit d'accès afin de protéger des intérêts prépondérants de tiers (par ex. en cachant le nom de l'auteur d'une analyse graphologique).

Enfin, se pose la question de savoir dans quelle mesure l'employeur peut *communiquer* des données concernant les employés *à des tiers*:

- l'employeur peut à coup sûr communiquer des données pour remplir une obligation prévue par la loi. Dans d'autres cas, la communication de données personnelles à des tiers peut se transformer aisément en violation de la personnalité et doit être pratiquée avec prudence, vu le devoir d'assistance qu'a l'employeur envers le travailleur.

- La pratique largement répandue consistant à octroyer à des tiers (par ex. bailleurs, organismes délivrant des cartes de crédit) des renseignements sur le revenu d'un travailleur sans obligation légale est contestable. Ce genre de renseignements doivent être recueillis par les tiers directement auprès de la personne concernée. Dans tous les cas, l'employeur ne doit les communiquer qu'avec l'accord du travailleur.

(Cf. ci-dessus à propos de la question de savoir si l'employeur peut communiquer des données à un autre futur employeur potentiel).

Après la fin des rapports de travail

A ce moment-là, une question se pose à tout employeur: que va-t-il faire des données dont il dispose sur son ex-employé ou employée?

- Conformément à l'article 328b CO, il n'est en droit de conserver que les données qui sont nécesssaires à l'exécution réglementaire du contrat de travail, même après son achèvement. En font partie les données qu'il doit conserver en vertu d'une obligation légale et les données dont la conservation relève de l'intérêt du travailleur (par ex. documents nécessaires à l'établissement d'un certificat, dans la mesure où il n'avait pas été déjà établi à la fin du rapport de travail). Les données qui ne sont jamais réutilisées doivent être immédiatement détruites (ce qui est également valable durant la valadité du contrat de travail).

- Pour les autres données dont on pourrait éventuellement avoir besoin, la durée de conservation sera déterminée dans chaque cas, en fonction de leur catégorie. En règle générale, on recommande une durée de conservation de 5 ans, qui exceptionnellement peut être prolongée à 10 ans, par exemple lorsque la loi le prévoit.

9.2. Administration fédérale

Le traitement des données du personnel de l'administration fédérale est en pleine mutation. PERIBU (système de gestion informatisé du personnel) est en cours de restructuration, des projets de traitement électronique décentralisé des données du personnel et de traitement électronique du temps de travail sont parallèlement à l'étude, des systèmes étant même opérationnels au sein de certains offices. Les "dossiers-papier" ne disparaîtront cependant pas tout à fait. Il est dès lors impérieux de réglementer "la cohabitation" de tous ces systèmes de traitement de données du personnel, et d'offrir aux personnes concernées un niveau de protection des données uniforme. Pour ce faire, l'élaboration d'une ordonnance du Conseil fédéral concernant la protection des données relatives aux agents de la Confédération est en cours. Cette réglementation se substituera à la circulaire de l'Office fédéral du personnel du 16 janvier 1984 concernant la protection des données relatives aux agents de la Confédération.

L'entrée en vigueur de la LPD a entraîné l'abrogation des Directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale. Ceci aurait dû également rendre caduque la circulaire de l'Office fédéral du personnel (OFPER) du 16 janvier 1984 concernant la protection des données relatives aux agents de la Confédération (ci-après la circulaire). Pourtant, l'OFPER a très justement estimé qu'il valait mieux maintenir cette circulaire en vigueur aussi longtemps qu'une ordonnance du Conseil fédéral spécifique à la protection des données relatives aux agents de la Confédération n'était pas adoptée. Une telle ordonnance, intitulée pour l'instant "projet d'ordonnance concernant la protection des données relatives aux agents de la Confédération" (ci-après l'ordonnance), est en cours d'élaboration. Le système PERIBU (système de gestion informatisé du personnel) est actuellement en voie de restructuration. Tant au sein du Département fédéral de justice et police (DFJP) que de celui de l'intérieur (DFI), des projets de traitement électronique des données (TED) du personnel et de traitement électronique du temps de travail (Muri 10 p. ex.) sont à l'étude, certains systèmes étant même opérationnels au sein de certains offices. Les données concernées par ces systèmes sont sensibles pour la plupart ou constitutives de profils de la personnalité. Une protection accrue de la personnalité des agents concernés est de ce fait requise. En outre, la plupart des informations actuellement contenues dans les "dossiers-papier" des services du personnel concernés seront reprises dans des systèmes TED, tels PIAS (DFJP) ou PISEDI (DFI), ce qui accroît d'autant plus les risques d'atteintes à la personnalité des agents de la Confédération concernés. L'ordonnance devra donc être aussi complète que possible, et contenir notamment des règles générales de protection des données (en reprenant, entre autres les dispositions contenues dans la circulaire), ainsi que des normes spécifiques aux dossiers du personnel et aux systèmes TED, ces normes devant également réglementer la "cohabitation" de tous ces systèmes entre eux. Nous allons vous faire part ci-dessous des idées-forces que nous avons exprimées tant

suite à l'examen de la première version de l'ordonnance que lors de l'analyse des projets TED qui nous ont été soumis.

Conservation des données relatives aux anciens candidats à un emploi: certains services du personnel dotés de systèmes TED propres ont pour pratique, en raison du fort taux de fluctuation de leur personnel, d'enregistrer et de conserver les données afférentes aux postulants dont les candidatures à un emploi n'ont pas été retenues. Ceci est fait dans l'éventualité où un tel candidat s'annoncerait une deuxième, voire une troisième fois à un poste. Cette pratique est contraire aux principes fondamentaux de la LPD (légalité, proportionnalité...) et à ce que prévoit la circulaire. Nous avons conseillé d'abandonner cette pratique et de l'interdire expressément dans l'ordonnance.

Egalité de traitement entre les agents qui quittent la Confédération et ceux qui passent dans une autre unité administrative: alors que le consentement de l'intéressé qui quitte la Confédération est requis avant qu'une communication de données le concernant (données du PERIBU ou de son dossier) soit effectuée à son nouvel employeur, ce n'est pas le cas lorsqu'un agent change d'unité administrative. Les données PERIBU sont alors sans autre directement rendues accessibles à la nouvelle unité. Cette solution est également envisagée dans certains projets TED, pour des agents changeant d'office au sein d'un même département, alors que les "dossiers-papier" ne sont jamais communiqués au nouvel employeur, que celui-ci soit ou non au sein de la Confédération, voire du même département. Nous avons ici recommandé que la procédure soit la même pour tous les agents, tant dans les cas de départ de la Confédération que de changement d'unité administrative, conformément aux principes généraux de protection des données et d'une saine gestion administrative. Le consentement des personnes concernées doit être systématiquement requis avant toute communication de données à des tiers, que le traitement des informations soit effectué par TED ou non. Quant au volume d'informations communiquées (données PERIBU par exemple), il doit être réduit au strict nécessaire. Nous avons finalement, au nom du principe de l'égalité de traitement, conseillé d'introduire, en annexe à l'ordonnance, un formulaire-type dans lequel le consentement à la communication ultérieure de données pourrait être requis de l'agent, indépendamment du fait qu'il quitte la Confédération ou change d'unité administrative.

Dispositions applicables aux systèmes de TED gérés de manière décentralisée par les unités administratives de la Confédération: nous avons ici recommandé d'introduire dans l'ordonnance des dispositions applicables à tous les systèmes TED du personnel existants et à venir, afin d'assurer un niveau de protection des données équivalent dans l'ensemble des services du personnel de la Confédération. Nous avons mis l'accent sur la nécessité de respecter les principes suivants dans tous les systèmes:

- obligation de constituer des systèmes fermés (Inselsysteme);
- limitation de l'accès aux systèmes aux seules personnes du service du personnel concerné habilitées à effectuer des mutations;
- remise périodique aux intéressés (chaque deux ans par exemple) d'un extrait compréhensible des données les concernant traitées dans le système. Le droit d'accès des agents doit également être possible sur demande;
- durée de conservation des données dans le système après le départ d'un agent la plus brève possible;

- transmission au nouvel employeur des seules données strictement nécessaires. Cette règle est également valable si l'agent change d'unité au sein d'un même département, doté du même système TED. L'informatisation des dossiers du personnel ne doit pas modifier les normes de communication de données régissant les "dossiers-papier". Or, ces derniers ne sont pas communiqués au nouvel employeur quel qu'il soit;
- versement aux Archives fédérales des seules données d'intérêt historique, cet intérêt devant être redéfini pour ce qui touche aux données relatives au personnel.

Dispositions applicables à PERIBU: nous avons ici recommandé à l'OFPER de compléter les dispositions de la section de l'ordonnance relative à PERIBU par les points suivants:
- mention des systèmes auxquels PERIBU est relié en ligne (online) et avec lesquels il y a un échange de données (le système SUPIS de la Caisse fédérale d'assurance par exemple), avec énumération des données échangées ou consultées;
- introduction, en annexe à l'ordonnance, du catalogue de données traitées dans PERIBU, sur le modèle de ce qui a été fait pour le système PISA du département militaire;
- obligation, pour tous les organes qui copient ou reprennent des données de PERIBU, de les tenir à jour et d'effacer de leurs systèmes TED les données auxquelles l'OFPER leur a retiré l'accès, notamment lors du départ ou du décès d'un agent.

Systèmes de calcul électronique du temps de travail (SET): nous avons ici insisté sur les éléments suivants:
- obligation de constituer les SET en systèmes fermés (Inselsysteme), reliés ni à PERIBU, ni à d'autres systèmes électroniques de traitement. Seule exception admissible: si un office emploie un nombre important d'agents payés à l'heure, une liaison en ligne avec PERIBU pourrrait être envisagée pour faciliter la gestion de leurs salaires;
- choix, pour la carte de légitimation, d'un numéro d'individualisation non signifiant au sens de la protection des données, et emploi de la même carte comme badge de timbrage;
- limitation de l'accès au SET aux seuls agents du service du personnel chargés des contrôles des opérations de timbrage et des mutations requises par lesdits contrôles;
- durée de conservation des données un an dans le système, puis sortie du système, stockage sur bandes magnétiques pendant deux ans, et destruction des données passé ce délai.

Consultation du personnel: nous avons constaté que ce principe, pourtant consacré dans la circulaire, ainsi que dans la Recommandation du Conseil de l'Europe concernant la protection des données à caractère personnel utilisées à des fins d'emploi, n'est à ce jour presque jamais respecté par les organes responsables de la création de fichiers du personnel. Nous avons attiré l'attention des services du personnel avec qui nous avons été en contact sur cette règle. Nous avons également recommandé de la consacrer dans l'ordonnance en ces termes:
"Lors de l'aménagement et de l'exploitation de fichiers manuels ou électroniques de données les concernant, les agents ou leurs représentants seront entendus."

"Dossiers-papier": nous avons exprimé ici l'avis qu'un contenu standard des dossiers devait être défini. Nous avons en outre recommandé d'introduire dans l'ordonnance le principe selon lequel tout acte concernant un agent doit être versé dans son dossier, l'intéressé recevant systématiquement copie d'un tel acte. Seule exception: la feuille d'appréciation, qui n'est, sauf cas conflictuel, accessible qu'à l'agent concerné et à son supérieur direct. Ceci implique qu'aucun exemplaire de cette feuille ne doit être versé au dossier, ni en original ni en copie. Nous avons constaté que la durée de conservation des dossiers des agents était excessive et qu'elle devait être ramenée de dix ans à cinq ans après la fin des rapports de travail. Quant au versement systématique des dossiers aux Archives fédérales passé ce délai, nous avons relevé qu'il ne correspondait ni à l'esprit du Règlement pour les archives fédérales, ni à la législation sur la protection des données.

Rôle du Préposé fédéral à la protection des données: vu que sa fonction de médiateur ne ressort plus clairement de la LPD, nous avons proposé, pour des raisons de transparence, de reprendre dans l'ordonnance l'idée déjà contenue dans la circulaire, qui pourrait être formulée en ces termes: "les agents peuvent demander conseil au Préposé fédéral à la protection des données ou requérir sa médiation".

L'informatisation croissante du traitement des données du personnel au sein de l'administration fédérale marque le début d'une ère nouvelle pour les agents chargés de la gestion de ces données. La technique offre des outils permettant en la matière une rationalisation optimale des tâches. La tentation est grande de ne prendre que des options techniques allant dans ce sens, au détriment de la personnalité des agents concernés. Or, l'administration fédérale se doit de privilégier le respect de la protection des données des intéressés, en renonçant si nécessaire à certains outils technologiques plus confortables, mais pas absoluments nécessaires à une saine gestion administrative. D'où certains choix qui devraient être pris dès le départ, telles la mise en place et l'exploitation de systèmes fermés (Inselsysteme).

10. Droit de bail

Formulaire d'inscription pour locataires

Suite à nos déclarations faites en décembre 1993 dans une émission de radio et aux réactions recueillies, nous avons établi à l'intention des bailleurs un rapport écrit analysant, sous l'angle de la protection des données, les questions figurant usuellement sur les formulaires d'inscription, et ce point par point. Il s'est avéré que la plupart des formulaires contenaient trop de questions, dont certaines n'étaient même pas nécessaires au choix du ou de la locataire.

Celui ou celle qui s'intéresse à un appartement doit dans la plupart des cas remplir un formulaire d'inscription et le remettre au propriétaire ou à la régie. Ces formulaires contiennent surtout des demandes de renseignements sur la personne même du locataire, sur sa situation financière et son domicile antérieur. Ces questions doivent permettre au bailleur de choisir entre plusieurs candidats. Le nombre des questions posées et leur contenu varient grandement selon les cas.

Nous avons examiné les questions posées dans les formulaires d'inscription du point de vue de leur compatibilité avec la LPD.

Conformément à l'article 13, 2e alinéa, lettre a LPD, les personnes privées peuvent traiter des données personnelles sur leur cocontractant lorsque ce traitement est en relation directe avec la conclusion ou l'exécution d'un contrat. Le bailleur a donc le droit de demander à celle ou celui qui s'intéresse à l'appartement en question des renseignements sur sa personne dans le but de signer un contrat de bail. Ces renseignements lui permettront de décider s'il veut conclure un tel contrat avec cette personne. Il ne doit toutefois les demander que s'il est sûr que la personne en question s'intéresse véritablement à l'appartement mis en location. Il serait par ailleurs disproportionné de demander aux personnes qui s'intéressent à un appartement de remplir le formulaire d'inscription avant d'avoir vu l'appartement à louer.

Le traitement de données personnelles en relation avec la conclusion d'un contrat n'est admis que si les principes généraux de la loi sur la protection des données sont respectés. Il convient en particulier de mentionner les principes de proportionnalité et de finalité auxquels les données relevées sont soumises.

La collecte de données, à propos de personnes s'intéressant à un appartement, sur un formulaire d'inscription est donc généralement admise. Nous sommes parvenus aux conclusions suivantes quant à l'ampleur d'une telle collecte:

le bailleur ne doit exiger des candidats que les données dont il a besoin pour choisir le locataire approprié selon des critères objectifs. Il a le devoir d'obtenir les renseignements dont il a besoin de la manière qui constitue pour le candidat l'atteinte minimum à sa personnalité. Si le bailleur est tenu de donner à certaines autorités des indications sur ses locataires, il ne doit collecter ces renseignements qu'à la conclusion du contrat. Enfin, il doit garantir que les données ne seront accessibles qu'aux personnes qui procèdent au choix du locataire, qu'il est impossible de traiter les données de manière non autorisée et que les données devenues inutiles seront immédiatement détruites.

Sur la base de ces considérations, nous avons établi une liste de données qui peuvent être normalement demandées (à savoir en l'absence de conditions objectives particulières). Cette liste est actuellement en procédure de consultation auprès des associations concernées. Au vu des résultats, nous établirons une liste définitive et prierons les bailleurs de se limiter aux données figurant sur cette liste lors de l'élaboration de leur formulaire d'inscription, à moins qu'ils puissent prouver objectivement leur besoin de renseignements supplémentaires. Nous publierons éventuellement une recommandation dans ce sens.

II. AUTRES THEMES

1. Ordonnance sur le relevé et le traitement des données relatives aux exploitations agricoles suisses

Signalons, à l'Office fédéral de l'agriculture, un exemple réjouissant de coopération dans le domaine de la protection des données entre l'administration fédérale et nous. Depuis plusieurs années, l'Office fédéral de l'agriculture travaille à l'élaboration d'un système d'information en vue de gérer rationnellement les données relatives à l'agriculture. Le système traite entre autres des données personnelles comme le nom, l'adresse et la profession de l'exploitant, le genre d'affectation agricole ou encore le nombre de personnes travaillant sur l'exploitation. Ce traitement de données a fait l'objet d'une base légale: l'ordonnance sur le relevé et le traitement des données relatives aux exploitations agricoles. Cette base légale garantit un traitement des données personnelles conforme à la législation sur la protection des données.

Ce système TED permet à l'Office fédéral de l'agriculture d'uniformiser le traitement des données de chaque exploitation (telles notamment l'adresse et l'emplacement de l'entreprise, sa forme d'organisation, la zone de production, le nom, l'adresse et la profession de l'exploitant, le genre d'affectation agricole, le nombre de personnes travaillant sur l'exploitation) dans le but de coordonner les relevés administratifs et statistiques. Ces données fournissent des informations sur toutes les entreprises agricoles de Suisse. Seules ou avec d'autres données relatives aux exploitations agricoles, elles permettent l'identification de l'exploitation ou de l'exploitant.

L'Office fédéral de l'agriculture a mis en place les bases légales nécessaires en collaboration avec nous. L'ordonnance qui règle désormais l'exploitation du système d'information (Système d'information de la politique agricole SIPA) a donc été conçue de manière à répondre aux principes de la protection des données. Il s'agissait notamment de fixer les conditions de transmission de données personnelles à d'autres autorités et les conditions d'accès par le biais du raccordement d'autres systèmes informatiques, ainsi que de réglementer dans l'ordonnance tous les traitements de données opérés au moyen de ce système, et de faire ainsi preuve de transparence à l'égard des citoyennes et citoyens.

2. Projet "Armée 95"

A partir du mois de juillet 1993, divers projets de révision d'actes législatifs nous ont été soumis par le Département militaire fédéral pour examen, dont le projet de loi sur l'armée et l'administration militaire. Dans ce projet, les bases légales des activités des services de renseignement et de sécurité militaire ont été créées. La base légale de PISA a quant à elle été complétée, afin que soient expressément mentionnés les organes bénéficiant d'une liaison en ligne à ce système.

3. Centre d'informations de crédit (ZEK)

Le ZEK a été fondé sous forme d'"Association pour la gestion d'un centre d'informations de crédit". Cette banque de données est un centre global des informations sur les débiteurs mis à disposition des membres de l'"Association suisse des banques de crédits et établissements de financement" (ASBCEF). Elle livre des

informations relatives à la solvabilité des demandeurs et bénéficiaires de crédits à la consommation et de leasings de biens de consommation.
Depuis l'entrée en vigueur de la LPD, nous sommes en contact avec le Secrétariat de l'ASBCEF, notamment pour les questions inhérentes à l'annonce du fichier ZEK et les modalités d'exercice du droit d'accès des personnes concernées. Le 9 mars 1994, nous nous sommes rendus au siège de l'AC Automation AG, qui met son centre de calcul à disposition de divers clients, dont les maîtres du fichier ZEK. Lors de cette première rencontre, nous avons procédé à un examen sommaire de l'environnement dans lequel se trouve le ZEK et de la mesure dans laquelle la sécurité des données est assurée.

4. Agences de renseignements commerciaux (Kreditauskunfteien)

Certaines de ces agences, dont Creditreform, sont en contact avec nos services depuis plusieurs années déjà. Depuis l'entrée en vigueur de la LPD, nous collaborons avec Creditreform sur les questions de devoirs d'annonce de fichiers et de flux transfrontières de données, ainsi que sur les modalités d'exercice du droit d'accès des personnes sujets de traitements de données. Cette entreprise fournit régulièrement des renseignements commerciaux à l'étranger, la plupart des destinataires de ces informations résidant dans des Etats qui ne disposent pas encore de législation sur la protection des données (p. ex. l'Italie), ou dont la loi n'est pas applicable aux personnes morales (dont l'Allemagne), ou encore qui ne sont dotés que de normes sectorielles de protection des données, tels les Etats-Unis. L'attention de Creditreform a été attirée sur le fait qu'elle devait s'assurer, selon la LPD, en particulier par voie contractuelle, que ses clients garantissent, pour les données qui leur sont livrées, un niveau de protection des données équivalent à celui de notre pays.

5. Registres privés de la propriété

Nous avons analysé dans quelle mesure la consultation par Telekiosk ou Vidéotex des registres privés de la propriété dans le cas de véhicules en leasing, volés ou saisis était admissible selon la LPD. Nous sommes arrivés à la conclusion que du point de vue du droit de la protection des données, de telles consultations sont admises pour autant qu'elles respectent certaines conditions.

Aujourd'hui, la consultation des registres privés de la propriété est possible par le biais du Telekiosk ou du Vidéotex. Ce genre de consultation est intéressant, notamment pour les acheteurs de voitures qui veulent s'assurer que le véhicule qui leur est offert à l'achat ne soit pas en leasing, saisi ou volé. Un exploitant d'un registre de la propriété nous a priés de prendre position à la lumière du droit de la protection des données. Selon les données de l'exploitant, le registre en question contient uniquement des données personnelles (numéro de téléphone et initiales du propriétaire du véhicule) que la personne concernée a transmises en sachant qu'elles pouvaient être utilisées ultérieurement. Aucune donnée personnelle concernant des tiers (p. ex. un preneur de leasing) n'est traitée, les contrôles de véhicules étant effectués sur la base du numéro de châssis. Du point de vue du droit de la protection des données, nous sommes d'avis que la mise à disposition de données personnelles figurant dans le registre de la propriété n'est pas problématique, dans la mesure où l'on prend soin de la confidentialité, de la

disponibilité et de l'exactitude des données traitées. Il en irait toutefois autrement si le registre était constitué de manière à permettre des interrogations par personnes, numéros de châssis, contenu des interrogations du système, etc. L'examen d'autres registres, notamment les registres de personnes visant à prévenir les pertes sur débiteurs, sera entrepris prochainement.

6. Mesures techniques et organisationnelles de protection des données

Une partie essentielle de la protection des données consiste en des mesures techniques et organisationnelles qui sont nécessaires pour assurer la transposition de la protection des données dans la pratique. Ces mesures sont présentées ci-après, ainsi que les expériences que nous avons acquises dans ce domaine au sein de l'administration fédérale.

L'article 7 LPD prévoit que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Bien que les exigences en matière de sécurité des données figurent déjà au chiffre 6 (organes fédéraux) des Directives du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale, force nous a été de constater, en particulier au sein de l'administration fédérale, que dans de nombreux cas, la sécurité des données ne faisait pas l'objet d'une attention suffisante. Ce problème est réglé à la section 4 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) du 14 juin 1993.

La protection des données requiert un système de traitement contrôlé de l'information, tel que le souhaite à vrai dire toute unité d'organisation ou toute entreprise. Pour des raisons de protection des données (mais aussi pour assurer une exécution efficace des tâches), chaque responsable, chaque unité d'organisation ou entreprise ne peuvent obtenir et traiter que les données personnelles nécessaires à l'accomplissement de leurs tâches.
Lors de la création de systèmes, il faut considérer dans une mesure équitable les intérêts des services spécialisés, des exploitants de systèmes et de la protection des données. Plus le traitement de données est sensible, plus il faut tenir compte des préoccupations de la protection des données.

Cette dernière soulève notamment les questions suivantes en relation avec la création (modification) de systèmes:

Quelles tâches accomplir avec quels moyens informatiques?
A cette question, on peut répondre en procédant à une analyse de l'organisation (analyse des tâches, analyse des besoins en informations, analyse des flux d'informations, etc.), de laquelle découlent notamment les besoins en données personnelles.
Chaque système d'information doit aider les responsables à exécuter leurs tâches. Dans ce but, il est nécessaire d'élaborer une documentation complète sur les tâches et les déroulements organisationnels nécessaires à leur accomplissement. Plus un système d'information est sensible, plus l'organisation de la structure et du déroulement doit être détaillée.

Quelles mesures (sécurité des données) techniques et organisationnelles nécessite un tel traitement de données personnelles?

- Lors de la transposition des mesures de sécurité, il est important de pouvoir couvrir les risques ou les dangers, avant tout par des mesures préventives (p. ex. dissociation des données personnelles des autres données; cloisonnement entre données personnelles et programmes; accès et possibilités d'exploiter uniquement les données (champs de données) jugées nécessaires à l'exécution des tâches; codage, etc.).
- Malheureusement, les mesures préventives ne suffisent pas toujours à garantir la protection des données. C'est pourquoi il est impératif de fixer l'exploitation courante dans les secteurs dans lesquels les mesures préventives ne satisfont pas aux exigences de la protection des données.
- En outre, il faut déterminer quel système prévalait à l'époque.

Le traitement informatique des données personnelles est-il légal?
- Lors de sa création, le système doit être adapté aux conditions-cadres légales, de telle sorte qu'il soit impossible ou presque, de déroger aux prescriptions. Dans ce but, il faut accorder la préférence à des mesures techniques contraignantes plutôt qu'à des dispositions d'ordre organisationnel, puisque dans la plupart des cas, de telles mesures empêchent de déroger aux prescriptions.

L'administration fédérale s'est vu accorder un délai transitoire de cinq ans pour transposer les mesures techniques et organisationnelles dans les systèmes existants. S'agissant de la création d'un nouveau système, il faut *prendre en compte dès le début* les exigences de la protection des données. On aboutit ainsi à un système de protection des données conforme et moins coûteux que le système dans lequel on introduit après coup les mesures de protection des données (dispositions techniques et organisationnelles).

Les expériences que nous avons pu récolter au sein de l'administration fédérale montrent que dans de nombreux cas, on ne tient pas encore suffisamment compte des exigences de la protection des données lors de la création de systèmes. Depuis l'entrée en vigueur de la loi sur la protection des données, les indications du genre "les prescriptions relatives à la protection des données doivent être respectées", que l'on rencontre dans les documents de planification des projets informatiques, sont devenues inacceptables; en effet, l'ordonnance relative à la loi fédérale sur la protection des données contient dans sa section 4 des objectifs qui indiquent clairement la manière dont il faut créer et exploiter un système pour garantir la protection des données. Afin de pouvoir se convaincre de la conformité d'un système avec la protection des données, il faut déterminer comment les constructeurs et exploitants de systèmes respectent les points de vue exposés dans l'art. 20 OLPD et en particulier les objectifs mentionnés à l'article 9, 1er alinéa, OLPD. Les constructeurs de systèmes doivent déterminer quelles mesures possibles ils prévoient pour atteindre ces objectifs. Il faut absolument mettre en évidence les différentes mesures avec leurs effets et les ressources y afférentes. Ce n'est que sur la base de ces informations transparentes que le maître du fichier pourra décider quelles dispositions il doit prévoir pour le système. A nos yeux, il est important de prendre une décision dont on puisse suivre le cheminement.

Nous constatons toujours et encore que *les tâches d'ordre organisationnel sont négligées au sein de l'administration fédérale*. Ce phénomène est d'autant plus étonnant que dans le cadre de la rationalisation des tâches ou de leurs processus

d'exécution, l'organisation joue un rôle prioritaire. Ce n'est qu'ensuite - surtout si l'on arrive à une solution qualitativement meilleure ou moins onéreuse - que l'on peut faire bénéficier ces processus du soutien informatique. Malheureusement, dans de nombreux cas, les aspects organisationnels ne sont pas assez documentés au sein de l'administration fédérale, même pour les systèmes sensibles, de sorte qu'il nous est difficile, voire impossible de déduire pour la protection des données les tâches qui sont exécutées dans les différents services ou unités d'organisation. Le peu de "soin" et le manque de documentation sur les besoins organisationnels ne constituent pas uniquement un problème pour la protection des données, mais aussi un problème entre les divisions spécialisées et l'informatique. Lorsque ces mêmes divisions sont dans l'incapacité de formuler leurs besoins, elles courent le danger de voir l'informatique développer un système qui ne tient qu'insuffisamment compte des processus d'exécution de leurs tâches. Compte tenu du fait qu'une bonne partie de la documentation relative à l'organisation fait défaut dans la plupart des cas, nous nous attachons momentanément à collecter les informations les plus importantes dans les unités d'organisation respectives. Malheureusement, nous constatons encore trop souvent que des réponses différentes sont apportées aux mêmes questions, *de sorte qu'à ce jour, il n'a pas été possible, sans la documentation nécessaire, de présenter une bonne analyse de la protection des données.*

D'où l'obligation pour les organisateurs et exploitants de systèmes de mieux tenir compte des conditions-cadres de la protection des données.
La responsabilité en matière de protection des données incombe au maître du fichier. Celui-ci devrait toujours se poser les questions suivantes:
Le traitement est-il légal?
Le système est-il organisé de manière transparente, donc contrôlable (règlement de traitement OLPD)? L'organisation (organisation de la structure et du déroulement) en particulier et les moyens informatiques bénéficient-ils d'une documentation suffisante?
Les mesures techniques et organisationnelles, nécessaires à la sécurité des données et chargées de garantir la protection des données, ont-elles été planifiées (mesures générales et particulières, journalisation OLPD)? Au sujet des mesures, les responsables ont-ils pris des décisions dont on peut suivre le cheminement? Ces décisions ont-elles aussi été transposées dans la pratique?
L'affectation du traitement des données aux seules fins prévues (principe de finalité) est-elle garantie?

7. Communication de données personnelles

7.1. Communication d'adresses par des organes fédéraux (article 19, 2e alinéa, LPD)

Les organes fédéraux sont souvent confrontés à des demandes de particuliers, d'associations ou d'entreprises désireuses d'obtenir les nom, prénom et adresse de personnes, que ce soit de manière individuelle ou sous forme de listes, dans un cas d'espèce ou de manière régulière et systématique. Les motivations de ces requêtes sont diverses. Elles peuvent être de nature idéale, économique et commerciale (notamment à des fins de publicité adressée) ou scientifique. Nous avons été appelés à nous prononcer à plusieurs reprises sur de telles demandes et avons pu ainsi dégager quelques lignes directrices.

L'article 19, 2e alinéa, LPD règle la communication des nom, prénom, adresse et date de naissance des personnes concernées. Cette disposition donne la faculté aux organes fédéraux de communiquer sur demande ces données, même si les conditions de l'article 19, 1er alinéa, LPD ne sont pas remplies. Ces conditions, alternatives, sont les suivantes: la communication est prévue dans une disposition légale, elle est dans un cas d'espèce indispensable à l'accomplissement de la tâche du destinataire, la personne concernée y a en l'espèce consenti ou son consentement peut être présumé au regard des circonstances, le destinataire rend vraisemblable que la personne concernée s'oppose à la communication pour échapper à une obligation juridique ou encore la personne concernée a rendu ses données accessibles à tout un chacun. *Il ne s'agit pas d'une obligation faite à l'organe fédéral requis, mais bien d'une faculté.* Il demeure en effet libre de communiquer ou non les données requises. Il doit néanmoins veiller à assurer l'égalité de traitement, à ne pas tomber dans l'arbitraire et à préserver les droits des personnes concernées. En particulier, l'organe fédéral doit s'abstenir de communiquer ces données si elles permettent de déduire d'autres informations sur les personnes concernées, notamment des informations sensibles au sens de la LPD. De même, la communication de ces données par procédure d'appel, notamment par un accès en ligne, demeure soumise aux exigences de l'article 19, 3e alinéa, LPD qui prévoit une base légale expresse. Enfin, la communication ne peut avoir lieu si la personne concernée s'y est opposée. Encore faut-il qu'elle rende vraisemblable un intérêt légitime et que l'organe communiquant ne doive pas lever l'opposition pour faire face à une obligation juridique ou pour accomplir sa tâche légale. L'organe responsable devra se montrer suffisamment large dans l'admission d'un intérêt de la personne à la non communication des nom, prénom, adresse et date de naissance. En outre, non seulement l'organe requis *peut*, mais *il doit* refuser la communication lorsqu'un important intérêt public ou un intérêt légitime manifeste de la personne concernée l'exige ou si une obligation légale de garder le secret ou une disposition particulière relevant de la protection des données le requiert (article 19, 4e alinéa, LPD).
La communication des nom, prénom, adresse et date de naissance ne peut intervenir que sur demande et dans un cas d'espèce, de manière isolée ou sous forme de liste. Par contre, une communication régulière et systématique de listes d'adresses ou la publication de telles listes ne sont pas couvertes par l'article 19, 2e alinéa.

7.2. Marketing direct

L'utilisation d'adresses à des fins publicitaires, sans l'accord de la personne concernée, est un procédé qui se répète des milliers de fois par jour en Suisse. Autant certains apprécient de recevoir de la publicité qu'ils n'ont pas commandée, autant d'autres sont dérangés par cette "irruption forcée dans leur sphère privée". Jusqu'à présent, nous n'avons pu malheureusement nous occuper de ce phénomène qu'à titre accessoire, mais nous l'étudierons prochainement dans le détail et tenterons, avec la collaboration des responsables de la branche, d'élaborer des solutions praticables.

Chez bon nombre de personnes concernées, l'utilisation d'adresses à des fins publicitaires se heurte à de la résistance et à du rejet. Certes, l'adresse n'est pas une donnée à caractère sensible; son traitement est autorisé aussi longtemps que la personne concernée ne l'a pas expressément interdit. Toutefois, il peut arriver qu'un envoi publicitaire non désiré porte atteinte à la personnalité, même gravement dans

certains cas (songeons par exemple à de la publicité à caractère pornographique distribuée à une personne vivant en couple).

La difficulté de garder la vue d'ensemble sur le traitement des données, et par conséquent *l'impossibilité de le contrôler* qui en découle, pose un problème particulier. Etant donné que l'on peut obtenir les adresses par les canaux les plus divers (PTT, communes, maisons d'expédition, bureaux d'adresses, listes des clients d'une entreprise, etc.), il est souvent impossible de déterminer l'origine d'un traitement d'adresses. Qui plus est, les possibilités à disposition (liste Robinson, blocage des adresses par les PTT) ne suffisent pas à juguler la distribution forcée d'envois publicitaires.

Dans une prise de position y relative, nous avons demandé à des responsables du marketing direct d'examiner la possibilité qu'aurait la personne concernée de remonter, à partir de l'adresse utilisée, jusqu'au maître du fichier (p. ex. par un code d'identification), afin de faire valoir son droit d'accès et, le cas échéant, d'exiger la rectification ou d'interdire l'utilisation de cette adresse. Dans le cas du traitement d'adresses à des fins publicitaires, il faut s'assurer déjà aujourd'hui que la personne concernée ne s'y oppose pas (p. ex. indication sur les formulaires d'annonce, information sur la vente d'adresses par les communes, etc.).

Nous nous sommes également exprimés sur l'admissibilité de la transmission d'adresses par des personnes privées à des fins publicitaires. Dans ce cas, le traitement des données a lieu d'après les principes généraux de la LPD, notamment le principe de finalité. Selon ce principe, les données ne peuvent pas être utilisées à des fins publicitaires lorsqu'elles ont été collectées dans un autre but et que la personne concernée n'a pas été informée de l'utilisation prévue ultérieurement. Encore faut-il que l'intéressé n'ait pas interdit la communication des données le concernant.

Nous prendrons prochainement contact avec les cercles concernés afin d'analyser dans le détail ce problème du marketing direct et de trouver des solutions praticables.

7.3. Communication de données personnelles des registres de détenteurs de véhicules automobiles

Appelés à donner notre avis au sujet d'un projet de modification d'une loi cantonale de protection des données tendant à introduire une disposition autorisant notamment la communication de données personnelles issues des fichiers des détenteurs et des conducteurs de véhicules automobiles à certaines entreprises du canton actives dans le domaine de la publicité adressée, nous avons estimé que le projet violait la liberté du commerce et de l'industrie et était contraire aux principes de finalité et de proportionnalité, ainsi qu'aux dispositions de la législation fédérale sur la circulation routière.

Selon le Tribunal fédéral, l'article 31 de la Constitution fédérale protège toute activité économique privée dirigée vers la production d'un gain et exercée à titre professionnel, soit toute activité déployée par une personne dans un but lucratif. Il couvre le droit de choisir et d'exercer librement toute activité lucrative privée, sur un point quelconque du territoire suisse. Aux termes de l'article 31, 2e alinéa cst, les

cantons peuvent restreindre la liberté du commerce et de l'industrie. Toutefois, ces restrictions doivent reposer sur une base légale, se justifier par un intérêt public prépondérant, respecter le principe de la proportionnalité, se conformer au principe de l'égalité de traitement des concurrents économiques et ne pas porter atteinte à la substance même de la liberté du commerce et de l'industrie. Les restrictions ne doivent pas être inspirées par des mesures de politique économique. Sont ainsi prohibées toutes mesures qui interviennent dans la libre concurrence pour assurer ou favoriser certaines branches de l'activité lucrative ou certaines formes d'exploitation et qui tendent à diriger l'activité économique selon un plan déterminé. Dans le cas d'espèce, la mesure envisagée, à savoir l'accès privilégié à certaines données des fichiers des conducteurs de véhicules, nous paraît clairement relever de la politique économique en faveur d'une branche particulière: la publicité adressée. L'accès privilégié est en outre limité à une ou deux entreprises de cette branche établies dans le canton. Cette mesure intervient dans la libre concurrence pour assurer ou favoriser une activité lucrative. Or, cette intervention est contraire à la jurisprudence du Tribunal fédéral. L'activité en question ne peut en outre être qualifiée d'activité d'intérêt public. Même si cela était, cet intérêt ne permet pas de chercher à intervenir dans le régime de la concurrence pour protéger certaines branches économiques ou formes d'entreprises contre la concurrence ou pour garantir leur existence. Une telle mesure est d'ailleurs contraire au principe de l'égalité de traitement. Enfin, elle ne respecte pas le principe de proportionnalité.

Nous avons souligné dans notre avis que, même si la mesure envisagée était jugée conforme à la liberté de commerce et de l'industrie et au principe de l'égalité de traitement, elle entrerait en conflit avec d'autres principes de la protection des données, notamment le principe de finalité, et avec la législation fédérale sur la circulation routière. Cette dernière régit en particulier la collecte de données relatives aux détenteurx et aux conducteurs de véhicules automobiles. Ces informations sont collectées par les cantons en exécution du droit fédéral et doivent être traitées ou communiquées conformément aux finalités pour lesquelles la législation fédérale sur la circulation routière l'autorise. Elles ne peuvent être utilisées à des fins qui ne sont pas en relation ou qui ne sont pas compatibles avec cette législation (par exemple à des fins de publicité directe ou à des fins fiscales autres que la taxation automobile). Les registres des détenteurs et des conducteurs de véhicules sont des registres de l'administration destinés principalement à lui servir d'instrument de travail. Ils ne sont pas publics. Certes, le droit de la circulation routière permet à certaines conditions de communiquer des données personnelles. Il autorise également les cantons à publier le registre des détenteurs de véhicules automobiles. Les personnes concernées bénéficient néanmoins du droit de bloquer la publication des données les concernant et par conséquent leur communication à des tiers si elles font valoir un intérêt légitime (l'exigence de l'intérêt ne doit pas être trop élevée). Nous avons d'ailleurs rappelé que cette possibilité de publication est critiquable sous l'angle de la protection des données.
Lorsqu'un canton publie le registre, nous avons finalement mis l'accent sur le fait que les finalités pour lesquelles le registre est publié doivent être compatibles avec les finalités pour lesquelles les données sont collectées. Cela exclut que les données puissent être communiquées à un destinataire particulier, de manière régulière et systématique, à des fins de publicité adressée.

8. Vidéosurveillance aux postes frontières

Dans le domaine de la sécurité intérieure, le contrôle des personnes franchissant les frontières joue un rôle important. Ce contrôle est effectué par les garde-frontières et les polices cantonales. Afin de rendre plus efficace la lutte contre l'immigration clandestine et les organisations de passeurs, l'administration fédérale des douanes envisage d'accroître les contrôles à la frontière verte, notamment en installant des caméras fixes ou mobiles aux endroits où des passages illicites sont fréquents et où il n'est pas possible de maintenir du personnel en permanence.

Depuis quelques années, les systèmes de télévision en circuit fermé sont entrés dans notre vie quotidienne, tant dans des établissements privés (banques, magasins, restaurants, lieux de travail, etc.), que dans des lieux publics (routes, frontières, places et bâtiments publics, stades, autres installations sportives ou culturelles). Le recours à la vidéosurveillance permet notamment de contrôler les spectateurs ou les participants à une manifestation sportive ou autre, de démasquer un client indélicat dans un magasin, de repérer un chauffard, un cambrioleur ou une personne franchissant illégalement une frontière. On utilise également ce moyen technique pour le contrôle des malades, la sécurité routière, celle des parkings ou d'autres installations, ou encore pour la surveillance de la production dans une entreprise. Toutes ces finalités sont le plus souvent légitimes. Pourtant, elles peuvent, à l'instar des écoutes téléphoniques, entraîner de graves atteintes à la personnalité et aux droits fondamentaux des personnes observées si certaines mesures ne sont pas respectées. Nous avons souligné que la vidéosurveillance est un moyen technique anonyme, parfois sournois et dont les conséquences peuvent être beaucoup plus graves pour l'individu qu'une simple surveillance visuelle effectuée par du personnel engagé à cet effet. Nous avons également rappelé que l'image relative à une personne ou qui permet son identification est une donnée personnelle. Dès lors, l'enregistrement et la conservation de ces informations, même pour un court laps de temps, constituent un traitement de données personnelles au sens de la LPD soumis aux principes généraux de cette loi.

Vidéosurveillance aux postes frontières: l'administration fédérale des douanes nous a fait part de son projet de recourir à ce moyen technique. Nous avons attiré son attention sur les points suivants:

licéité de l'enregistrement. En tant qu'organe fédéral, l'administration des douanes doit fonder son recours à la vidéosurveillance sur une base légale suffisante. Nous avons jugé une ordonnance du Conseil fédéral suffisante dans la mesure où l'installation n'implique pas d'enregistrements et de conservation (au-delà de quelques jours) des données et où la vidéosurveillance n'a pas lieu à l'insu des personnes concernées. Par contre une conservation pour plusieurs semaines, voire mois ou années permettant d'utiliser les données au-delà de ce qui est nécessaire à la surveillance frontière immédiate, notamment en communiquant les données à d'autres autorités fédérales ou cantonales nécessiterait une base légale dans une loi au sens formel, dans la mesure où une telle conservation ou utilisation multiple seraient indispensables;

traitement de l'information conforme au principe de la *bonne foi.* Les personnes filmées doivent en principe être au courant de la mesure de surveillance et les caméras devraient être visibles afin de permettre à la personne concernée d'adapter son comportement à la situation, et de renoncer le cas échéant à pénétrer dans un

établissement doté d'un tel système. Si l'information ne peut être donnée préalablement, elle doit l'être ultérieurement. Dans le cas d'espèce, nous avons cependant admis que l'administration fédérale des douanes puisse cacher ses caméras pour des raisons stratégiques. Nous nous sommes ralliés au point de vue de cette administration pour ce qui touche à l'emploi d'installations mobiles, dans la mesure où les douaniers eux-mêmes peuvent se cacher pour observer la frontière verte et pour autant que les informations ainsi collectées ne soient pas conservées au-delà de 24 heures, dans les cas où aucune interpellation n'a été opérée. Par contre, comme pour les douaniers employés à un poste frontière, nous avons estimé que les installations fixes devaient rester visibles, ou dans le cas contraire, nous avons recommandé d'informer par voie d'affichage les personnes concernées du fait que la zone frontalière se trouve sous vidéosurveillance;

respect du principe de *proportionnalité.* On ne recourt à la vidéosurveillance que si ce moyen est indispensable à atteindre le but visé et que la surveillance ne peut être exercée efficacement par des moyens moins attentatoires à la personnalité et aux droits fondamentaux. L'enregistrement et la conservation de l'information ne sont admissibles que dans les limites nécessaires aux tâches pour lesquelles la vidéosurveillance doit être exercée. Dans le cas de la surveillance aux frontières, les enregistrements ne devraient pas être conservés si aucune infraction ou situation irrégulière n'ont été immédiatement constatées. Dans ce sens nous avons considéré que le délai de 24 heures prévu par les douanes suisses était adéquat;

conformité du recours à la vidéosurveillance au principe de *finalité*. Ce moyen doit être introduit en vue d'une tâche déterminée et ne pas permettre de collecter des données de manière illimitée et pour des finalités indéfinies. Dans le cadre des douanes, nous avons conseillé de limiter la vidéosurveillance au contrôle du passage de la frontière, notamment en vue d'empêcher que des illégaux s'introduisent sur le territoire et permettre de lutter contre les passeurs.

III. APPLICABILITE DE LA LPD AU NIVEAU CANTONAL

La loi fédérale sur la protection des données est applicable au traitement de données personnelles par des personnes privées et des organes fédéraux. Elle n'est en principe pas applicable au traitement de données par les autorités cantonales. Mais en vertu de l'article 37 LPD, il en va néanmoins autrement lorsque les cantons remplissent des tâches de la Confédération, dans la mesure où il n'existe pas au niveau cantonal de prescriptions sur la protection des données. Dans ce contexte, la question se pose de savoir quelles sont les exigences auxquelles les dispositions cantonales de protection des données doivent satisfaire pour que la loi fédérale sur la protection des données ne soit pas applicable.

La protection des données découlant de droits constitutionnels, notamment de la protection du droit non écrit de la liberté personnelle, ainsi que du principe d'égalité de traitement en vertu de l'article 4 de la Constitution fédérale, les cantons doivent de ce fait satisfaire à des exigences minimales d'ordre constitutionnel, quant au traitement de données personnelles qu'ils effectuent. Par ailleurs, dans le domaine de l'activité administrative cantonale, les cantons disposent de leur autonomie d'organisation. Ils sont donc libres d'édicter des règles sur les traitements de

données personnelles dans l'administration publique et communale. Mais du fait que les cantons, de par leur activité administrative, non seulement règlent leurs propres tâches, mais exécutent aussi du droit fédéral, des divergences risquent d'apparaître entre la protection des données au niveau cantonal en exécution du droit fédéral et la protection des données au niveau fédéral.

L'article 37 a été intégré dans la loi sur la protection des données afin de garantir une certaine uniformité des traitements de données effectués par les organes fédéraux et par les organes cantonaux dans l'exécution du droit fédéral, et essentiellement en vue de l'éventuelle ratification de la Convention no 108 du Conseil de l'Europe "pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel".

L'article 37 LPD ne peut produire ses effets que si les cantons exécutent du droit fédéral. Il n'est pas toujours facile de distinguer les cas où les cantons exécutent du droit fédéral de ceux où ils exécutent du droit cantonal. A ce propos, il convient de souligner essentiellement deux points :

- la frontière entre l'exécution de ce qui est encore du droit cantonal - en d'autres termes lorsque les cantons accomplissent une tâche à l'origine cantonale - et l'exécution de ce qui relève déjà du droit fédéral n'est pas toujours bien définie;
- les organes cantonaux assument parfois, par exemple dans le domaine fiscal, en même temps des tâches d'exécution cantonales et fédérales. L'accomplissement des tâches fédérales et cantonales fait dans certains cas l'objet d'une même procédure et se déroule sur la base des mêmes documents. Presque toutes les données reprises et traitées sont importantes tant pour l'exécution des lois fédérales que pour l'exécution des lois cantonales. Il convient alors de délimiter si c'est le droit de la protection des données de la Confédération ou celui du canton qui est applicable. A ce propos, les administrations cantonales sont soumises à diverses législations sur la protection des données en ce qui concerne une seule et même activité administrative.

Ce que l'on entend par "disposition cantonale de protection des données" revêt de ce fait une importance fondamentale à propos de l'article 37, 1er alinéa, LPD. On ne peut dégager de la loi aucun critère quant à la *qualité formelle* des dispositions cantonales. Le législateur a renoncé à établir définitivement si les dispositions cantonales de protection des données doivent revêtir la forme d'une loi au sens formel ou si une ordonnance suffit. Il ne voulait pas obliger les cantons à créer des normes juridiques équivalentes à la loi fédérale sur la protection des données. Au cours des débats parlementaires, l'unanimité régnait néanmoins à propos du fait que les dispositions du droit cantonal de protection des données doivent avoir un caractère normatif. Les normes doivent avoir l'effet de règles déterminantes pour le juge. Elles doivent déployer des effets vis-à-vis des tiers. Sous l'angle de la Convention du Conseil de l'Europe et de la problématique des droits fondamentaux, nous sommes d'avis que par "dispositions cantonales de protection des données" au sens de l'article 37, 1er alinéa, LPD, on doit entendre *les actes juridiques ayant forme de loi*.

De même pour ce qui est du *contenu matériel* des dispositions cantonales, le législateur n'a pas voulu imposer aux cantons des exigences susceptibles de générer

de considérables divergences, par exemple quant aux droits de la personne concernée, entre la loi fédérale sur la protection des données et les dispositions cantonales. Cependant, étant donné que la protection des données relève de la protection de la personnalité et des droits fondamentaux, il faut d'une part au moins interpréter les exigences issues de l'abondante jurisprudence du Tribunal fédéral - notamment à propos du droit fondamental à la liberté personnelle et de l'article 4 Cst. - comme un standard minimal que les dispositions cantonales de protection des données doivent offrir. D'autre part, surtout du point de vue matériel, il convient de mettre en oeuvre la LPD comme une directive ou un modèle. Ainsi que l'avait prévu la loi-modèle sur la protection des données présentée à l'occasion de la Conférence des chefs des départements cantonaux de justice et police en 1983, il faut que les dispositions cantonales contiennent aussi des normes minimales dans l'optique de la Convention du Conseil de l'Europe.

Conformément à l'article 37, 2e alinéa, LPD, les cantons désignent un organe chargé de veiller au respect de la protection des données. Les articles 27, 30 et 31 sont applicables par analogie. D'aucuns estiment que l'alinéa 2 n'est applicable que lorsque les tâches cantonales d'exécution du droit fédéral sont soumises à la LPD, en l'absence de dispositions cantonales de protection des données au sens de l'article 37, 1er alinéa, LPD. Ce ne serait que dans ce cas que les cantons devraient constituer leur propre organe de protection des données. Cette opinion est juste si l'on part du principe que les dispositions cantonales de protection des données doivent fixer des contenus minimaux, notamment prévoir un organe de contrôle tel que l'exige l'article 37, 2e alinéa, LPD. On peut néanmoins imaginer que des dispositions cantonales actuelles de protection des données, soit ne prévoient aucun organe de contrôle, soit renferment des règles relatives à des organes de surveillance qui ne répondent aucunement aux exigences posées à un organe de contrôle au sens de l'article 37, 2e alinéa, LPD. Nous sommes donc d'avis qu'indépendamment de l'existence de dispositions cantonales de protection des données, les cantons sont tenus de mettre en place un organe de contrôle au sens de l'article 37, 2e alinéa, LPD.

L'organe de contrôle au sens de l'article 37, 2e alinéa, LPD doit être à notre avis *une instance neutre et indépendante* à laquelle les participants - maîtres des fichiers, personnes concernées - peuvent faire appel en cas de litige. Par ailleurs, pour assurer l'uniformité du contrôle, nous estimons que seule entre en ligne de compte une *instance centrale unique* surveillant objectivement le respect des règles de protection des données.

Les articles 27, 30 et 31 LPD sont applicables par analogie aux *tâches et aux compétences de l'organe de contrôle* qu'il convient de désigner. En d'autres termes, il est possible mais non obligatoire d'appliquer les dispositions de la LPD. Il convient plutôt selon les cas de tenir compte des circonstances qui règnent dans le canton en question et du système qui y est appliqué, c'est-à-dire de la structure et de l'organisation de chaque canton. Par ailleurs, il faut toujours tenir compte de l'autonomie d'organisation dont les cantons jouissent en principe. Les articles 27, 30 et 31 ne doivent donc pas être considérés comme normes minimales. Il serait opportun à ce propos que les cantons mettent en place dans leur propre intérêt des conditions semblables à celles prévues par la LPD, par exemple en son article 31, 2e alinéa.

IV. ACTIVITES INTERNATIONALES

Les problèmes liés à la protection des données ne s'arrêtent pas aux frontières nationales. Dans un monde de plus en plus interdépendant et technologiquement toujours plus performant, les échanges d'informations et notamment d'informations personnelles au-delà des frontières nationales sont devenus banals et répondent à des nécessités diverses quelles soient économiques, scientifiques, culturelles, touristiques, administratives ou policières. Cette dimension internationale des flux de données personnelles peut affaiblir le système national de protection des données et rend indispensables une harmonisation du droit et une coopération internationale.

La LPD prévoit expressément que nous avons en particulier pour tâches de collaborer avec les autorités chargées de la protection des données à l'étranger et d'examiner la mesure dans laquelle le niveau de protection des données assuré à l'étranger est équivalent à celui que connaît la Suisse. Cette collaboration est indispensable dès lors que la plupart des activités nécessitant le traitement de données personnelles débordent les frontières nationales et que les problèmes de protection des données ne se limitent pas à une région ou à un Etat donné. Elle permet notamment d'échanger des informations, de dégager des solutions communes entre autorités de protection des données, de conseiller les personnes et organes traitant des données personnelles et d'assister les personnes concernées dans l'exercice de leurs droits à l'étranger. Cette collaboration s'opère à différents niveaux: contacts bilatéraux, Conférence internationale des Commissaires à la protection des données, Organisations internationales (notamment, Conseil de l'Europe et OCDE).

1. Conférence Internationale des Commissaires à la protection des données

Les instances de contrôle de la protection des données prévues par différentes législations nationales 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 harmoniser leurs pratiques, et le cas échéant d'adopter des positions communes (résolution de la Conférence).
La XVe Conférence Internationale des Commissaires à la Protection des données s'est déroulée à Manchester du 27 au 30 septembre 1993, à l'invitation du "Data Registrar" du Royaume-Uni. La Conférence a permis de faire le point sur le développement international de la protection des donnéees. Elle a également été l'occasion d'un échange de vues approfondi sur les problèmes de la collecte de données personnelles provenant de fichiers publics et notamment leur utilisation à des fins commerciales, le respect de la vie privée et de la liberté d'expression, le recours à des identifiants (numéro d'identification, marquage génétique), le recensement de la population, la surveillance notamment à l'aide d'installations vidéo ou encore la sécurité informatique. Face aux nouveaux moyens d'investigations que la technologie moderne met à notre disposition (dépistage génétique, vidéosurveillance, surveillance électronique, ...), les Commissaires à la protection des données ont mis l'accent sur la nécessité de trouver un juste équilibre entre le besoin d'informations et le respect des droits fondamentaux et notamment de la vie privée. Ils ont estimé qu'il convenait de bien faire la balance entre le bénéfice que

ces moyens peuvent apporter et les limitations des droits des individus, ainsi que les conséquences de ces limitations sur nos sociétés démocratiques.

2. Conseil de l'Europe

Depuis plus de vingt ans, le Conseil de l'Europe se préoccupe de l'harmonisation du droit de la protection des données en Europe et mène des travaux en ce sens. En 1981, il a adopté et ouvert à la signature de ses Etats membres la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Cette Convention a été ratifiée par quinze Etats (Autriche, Belgique, Danemark, Finlande, France, Allemagne, Islande, Irlande, Luxembourg, Pays-Bas, Norvège, Portugal, Espagne, Suède et Royaume-Uni). Six autres Etats (Chypre, Grèce, Hongrie, Italie, Slovénie et Turquie) l'ont également signée. Jusqu'à l'entrée en vigueur de la LPD notre pays n'était pas en mesure de signer, ni de ratifier cette Convention. Bien que tous les cantons n'aient pas encore adopté de loi sur la protection des données, nous estimons que le moment est venu pour notre pays de ratifier ce texte, et le 14 juin 1993, le Conseil fédéral a confié le mandat au DFJP de préparer le message y relatif.
Au sein du Conseil de l'Europe, deux comités sont chargés des questions de protection des données. Il s'agit tout d'abord, du Groupe de projet sur la protection des données du Conseil de l'Europe (CJ-PD), auquel nous participons activement et qui se réunit deux fois l'an en plénum. Le CJ-PD élabore en particulier des recommandations concrétisant et précisant les principes généraux de la Convention 108 dans des secteurs particuliers. Huit recommandations (banques de données médicales, recherche scientifique et statistique, marketing direct, sécurité sociale, police, emploi, fichiers publics, opérations de paiement et autres opérations connexes) ont été adoptées depuis 1981. Actuellement, quatre autres recommandations sont en préparation et portent sur les télécommunications, les données médicales (et notamment recherche médicale, génétique), la statistique et les assurances. En outre, le CJ-PD examine l'opportunité de réviser et compléter la recommandation sur la police pour tenir compte notamment des systèmes d'informations transfrontières (tels les systèmes Shengen ou Europol).
Un autre comité est également actif en matière de protection des données. Il s'agit du Comité consultatif prévu par la Convention 108, chargé en particulier de donner des avis sur l'application de ladite Convention. Ce comité, auquel nous prenons part en tant qu'observateurs, se réunit une à deux fois l'an. En 1993, il s'est notamment attelé à finaliser un projet de contrat-type en matière de flux transfrontières de données élaboré en collaboration avec l'Union européenne et la Chambre de commerce internationale. Le but de ces clauses est d'assurer par voie contractuelle le respect des principes de la Convention 108 en cas de transfert de données vers des Etats n'ayant pas ratifié cette dernière. Ce comité a en outre entamé une réflexion sur les questions de savoir si les informations relatives aux personnes décédées, ainsi que l'image et la voix des personnes physiques sont couvertes par la protection des données, respectivement la Convention 108. Il n'a à ce stade pas encore pris de conclusions définitives. Enfin, il examine les conditions auxquelles l'Union européenne pourrait ratifier la Convention 108, comme elle en a manifesté l'intention.

3. Organisation de coopération et de développement économique (OCDE)

L'OCDE est également active dans le domaine de la protection des données. Cette organisation a en particulier adopté le 23 septembre 1980 des Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. Ces lignes directrices, à l'instar de la Convention 108, visent à harmoniser le droit de la protection des données, notamment en vue de garantir le libre flux des informations. Elle fait l'objet d'un suivi sous forme de réunions ad'hoc d'experts des différents Etats membres. Ces réunions permettent de faire un bilan sur l'évolution du droit de la protection des données dans les différents Etats membres et d'examiner certains problèmes particuliers (par exemple, flux transfrontières de données, télécommunications, cartes de crédit, vidéosurveillance, ...). C'est ainsi qu'en 1993, ces experts se sont réunis et se sont plus particulièrement penchés sur les problèmes de protection des données dans le cadre des dossiers médicaux et de la recherche médicale. Cette réunion a permis un large échange de vue sur les différentes politiques nationales relatives au traitement de données médicales. C'est ainsi que la solution suisse d'instaurer une Commission d'experts sur le secret professionnel en matière de recherche médicale chargée de délivrer des autorisations de communiquer des données médicales a reçu un écho favorable de la part des autres délégations. Cette solution a également été retenue dans le projet de recommandation du Conseil de l'Europe actuellement discuté par le CJ-PD. D'autres solutions ont également été préconisées, notamment celles permettant d'effectuer des recherches médicales sans que les chercheurs aient connaissance de l'identité des personnes (anonymisation, moyens de cryptographie des informations, codage des identifiants, utilisation de pseudonymes).

4. Union européenne

La Commission de la Communauté européenne a présenté en septembre 1990 un projet de directive relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Suite à une vaste procédure de consultation, notamment auprès des institutions communautaires, des Etats membres, des Commissaires à la protection des données et des milieux privés intéressés, un deuxième projet remanié a été présenté en octobre 1992 et est actuellement discuté au sein du Conseil de l'Union européenne. D'autre part, l'Union européenne étudie un 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.

5. Contacts bilatéraux

Durant la phase introductive de la loi, nous nous sommes adressés à plusieurs reprises aux autorités de protection des données de différents Etats européens pour obtenir des informations sur leur organisation. D'autre part, nous les avons consultés sur des questions particulières touchant principalement aux domaines de la police, des écoutes téléphoniques ou des nouvelles technologies (RNIS, X.500). Nous avons également répondu à deux demandes d'entraide de l'Allemagne et de la France, qui toutes deux avaient trait au marketing direct. Le premier cas portait sur

une campagne de publicité par fax qui avait fait l'objet d'une plainte d'un particulier en Allemagne fédérale. Le Commissaire fédéral allemand a requis notre aide pour savoir de quelle manière la firme suisse qui avait mené cette campagne détenait les données relatives à la plaignante et quelles informations la concernant elle traitait. Nos éclaircissements ont abouti au constat que la firme en question utilisait simplement un annuaire de numéros de fax et qu'elle ne conservait aucune information sur les personnes auxquelles elle envoyait ses messages.
Le deuxième cas est encore en cours d'instruction. La Commission nationale de l'Informatique et des Libertés nous a consultés au sujet d'une plainte d'une entreprise française qui recevait à titre de publicité des factures à des fins d'inscription dans un annuaire international.

V. REGISTRE DES FICHIERS

Le registre des fichiers de données personnelles vise avant tout à informer le public des trai-**tements de données personnelles effectués par les organes fédéraux et les personnes privées. La LPD requiert des organes fédéraux qu'ils nous déclarent tous leurs fichiers de données personnelles, et des maîtres de fichiers privés qu'ils annoncent ceux de leurs fichiers qui remplissent les conditions prévues par la LPD. Après examen sommaire des formulaires de déclaration par nos soins, les informations ainsi collectées seront introduites dans un système de gestion électronique du registre des fichiers (DATAREG). Cet instrument nous permettra d'assurer la publication périodique de ce registre, servira d'instrument de contrôle, ainsi que de source d'informations pour les personnes désireuses d'exercer leur droit d'accès. Près de 1'500 déclarations de fichiers sont attendues.**

Ce registre a été publié deux fois, la dernière fois en 1991 (état au 1er mars 1990), conformément aux Directives du Conseil fédéral du 16 mars 1981 applicables au traitement des données personnelles dans l'administration fédérale. Il ne contenait que les fichiers de données personnelles détenus par les services de l'administration fédérale. Depuis le 1er juillet 1993, les personnes privées dont les fichiers remplissent les conditions posées par la LPD sont également soumises au devoir de déclaration. Cette dernière devra avoir été faite d'ici au 30 juin 1994 auprès de notre Secrétariat, au sein duquel un petit groupe de travail examine sommairement le contenu des annonces. Le développement d'un système de traitement électronique du registre des fichiers est sur le point d'être achevé (DATAREG). Cet instrument devrait nous permettre de gérer efficacement les quelque 1000 annonces provenant de l'administration, ainsi que les 500 déclarations environ que nous attendons du secteur privé.

1. Buts du registre

Le registre des fichiers vise à informer le public des traitements de données personnelles effectués par les organes fédéraux et les personnes privées. C'est un instrument destiné à assurer la publicité des fichiers, afin notamment de faciliter, pour les personnes concernées, l'exercice de leur droit d'accès. Le registre indique qui traite des données et dans quelle mesure. Il mentionne finalement, pour chaque

fichier publié, l'organe à qui adresser une demande d'accès. Le registre nous sert en outre d'auxiliaire dans l'accomplissement de nos tâches de conseil et de contrôle.

2. DATAREG - Système de gestion du registre des fichiers

L'ancien registre des fichiers de données personnelles contient près de 600 saisies de fichiers de données personnelles de l'administration fédérale. Créé à l'origine dans le but de faciliter l'exercice du droit d'accès, il est exploité comme un "fichier-texte" dans les langues allemande, française et italienne. Les dernières modifications n'y ont pas été reportées.

D'après la LPD, les organes fédéraux sont tenus de déclarer tous leurs fichiers. Sous certaines conditions, les personnes privées doivent elles aussi désormais se conformer à cette disposition. Ainsi, nous aurons à l'avenir deux registres de fichiers dans les langues allemande, française et italienne: l'un pour les fichiers des organes fédéraux, l'autre pour ceux des personnes privées. La déclaration a lieu au moyen de formulaires ad hoc que nous délivrons. L'acceptation de la déclaration et l'enregistrement des fichiers dans le registre ne signifient rien quant à la légitimité du traitement des données dans le fichier concerné.

La gestion des saisies de données est assurée par un logiciel développé à cet effet: DATAREG. L'application est basée sur une banque de données relationnelle, qui facilite la gestion et la mise à jour des entrées dans le registre. DATAREG permet la saisie des entrées et leur numérotation automatique. Toutes les annonces sont enregistrées dans le registre, mais elles ne seront pas toutes publiées. La saisie s'effectue en trois langues. La langue originale est indiquée dans le code langue des entrées des déclarations du fichier. Les trois saisies forment logiquement une unité. L'utilisation de catalogues trilingues de termes permet de réduire aussi bien le travail de saisie que les possibilités d'erreur. Cette méthode garantit également l'unité de doctrine pour la traduction d'un mot. Par ailleurs, elle permet de vérifier la concordance de la traduction et de l'original et d'exclure dans la mesure du possible les erreurs. Toute modification des données individuelles dans les saisies des données du registre entraîne automatiquement une mise à jour de toutes les entrées concernées. A ce sujet, on a pris garde d'éviter au maximum les redondances. En outre, différentes fonctions de recherche et d'exploitation ont été intégrées. Elles seront encore étendues selon les besoins.

Le registre des fichiers est publié. La publication des données tirées de DATAREG doit si possible s'effectuer sans intervention manuelle. Les fonctions y relatives seront opérationnelles d'ici le début 1995. D'ici-là, toutes les déclarations devraient également être saisies dans le système de gestion. La publication des entrées des déclarations des organes fédéraux correspondra dans sa forme au registre actuel des fichiers de données personnelles.
Quant au registre des entrées des déclarations des personnes privées, il sera structuré par ordre alphabétique et, au sein d'une branche, d'après le nom des entreprises.

A l'avenir, compte tenu de la fréquence des prochaines publications et des expériences acquises, on pourrait prévoir d'engager des moyens supplémentaires pour la déclaration des fichiers et la publication du registre des fichiers. On pense ici

en particulier aussi bien à des supports électroniques de données qu'à des équipements de transmission de données et à des services de télécommunications.

3. Formulaires de déclaration

Nous avons établi quatre types de formulaires, dont deux visent à alimenter le registre des fichiers, à savoir:

le formulaire de déclaration de fichiers gérés par les organes fédéraux: le même formulaire étant utilisé tant pour les annonces ordinaires que pour les annonces simplifiées ou globales. Ce formulaire contient notamment les nom et adresse de l'organe fédéral responsable, le nom et la denomination du fichier, l'organe auprès duquel peut être exercé le droit d'accès, la base juridique et le but du fichier, les catégories de données traitées, de destinataires des données et de participants au fichier, ainsi que le cercle des personnes concernées et leur nombre approximatif;

le formulaire de déclaration de fichiers gérés par des maîtres de fichiers privés: les informations requises sont les mêmes, à l'exclusion de la base juridique, ainsi que du cercle des personnes concernées et de leur nombre approximatif;

le formulaire de déclaration de flux transfrontières de données à l'usage des organes fédéraux: ce dernier n'est pas rempli à des fins de publication, mais pour que nous puissions contrôler que lors de communications de données à l'étranger, un niveau de protection des données équivalent à celui de notre pays soit assuré;

le formulaire de déclaration de flux transfrontières de données à l'usage des maîtres de fichiers privés: ce formulaire vise le même but que le précédent.

4. Premières expériences

En mars 1994, nous avions reçu environ une centaine d'annonces, dont un tiers émanant du secteur privé. Les organes fédéraux ont des difficultés à organiser efficacement la procédure de déclaration de leurs fichiers. Les formulaires d'annonces doivent dans près de 90% des cas être retournés pour correction ou complément. Dans le domaine des assurances sociales, les caisses d'assurance en particulier, que la LPD considère comme des organes fédéraux lorsqu'elles exécutent une tâche de la Confédération, sont confrontées pour la première fois au devoir devoir d'annonce. Ces caisses ne peuvent pas toujours déterminer si elles sont soumises au devoir de déclaration auprès des organes cantonaux de protection des données ou auprès de notre Secrétariat.
Dans le secteur privé, les annonces proviennent pour l'instant essentiellement d'entreprises actives dans le domaine de l'adressage (marketing direct). Ici également, les formulaires doivent être fréquement retournés pour complément. D'autres secteurs d'activité se sont adressés à notre Secrétariat pour une future déclaration. Il s'agit notamment d'agences de renseignements commerciaux et de compagnies d'assurances. Nous aimerions finalement souligner que les maîtres de fichiers privés remplissent volontiers leurs obligations légales.

Le registre des fichiers de données personnelles est un instrument indispensable pour permettre aux personnes sujets de traitements de données d'exercer leur droit d'accès. Il facilite également l'accomplissement de nos tâches légales. Pour être performant, le registre doit cependant être aussi fiable et complet que possible. Il requiert donc, tant de la part des maîtres de fichiers que de notre part, un travail soigneux et de longue haleine. De ce fait, la publication de cette nouvelle version du registre des fichiers ne pourra pas avoir lieu avant 1995.

VI. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

Si l'on veut se remettre à l'esprit ce qu'est le Secrétariat du PFPD, il est utile de rappeler brièvement quelles sont ses activités. Selon la loi sur la protection des données, le Secrétariat conseille et surveille tous les organes fédéraux de notre pays, soit plusieurs milliers de collaborateurs, dans les questions relatives à la protection des données, notamment en ce qui concerne les projets législatifs et les projets TED. Par ailleurs, il conseille et contrôle l'ensemble du secteur privé, c'est-à-dire toutes les personnes privées qui, en Suisse, traitent d'une manière ou d'une autre des données personnelles. Finalement, il est chargé de sauvegarder les intérêts des citoyennes et des citoyens, puisque toute personne concernée a la possibilité de s'adresser au PFPD en cas de problèmes ou de questions en rapport avec l'attitude des organes fédéraux ou des personnes privées à l'égard de ses données. D'autres tâches du PFPD sont: l'information (présenter des exposés, organiser et mener des réunions et des conférences, créer et mettre à disposition du matériel d'information tel que aide-mémoire, guides, brochures relatives au traitement de données personnelles); la rédaction du rapport d'activités; la création, la gestion et la publication du registre des fichiers; la collaboration avec les autorités suisses et étrangères de protection des données; l'examen de l'équivalence des lois étrangères sur la protection des données; la représentation de la Suisse dans des comités internationaux (Conseil de l'Europe); les activités de conseil de la Commission d'experts du secret professionnel en matière de recherche médicale, l'examen des décisions de cette commission et l'information des patients sur leurs droits.
Pour toutes ces tâches, le PFPD ne dispose que de 9,3 postes (2 postes supplémentaires ont été accordés pour avril de cette année). Une exécution soignée, voire satisfaisante de toutes ces tâches est impossible avec des moyens en personnel aussi limités.

1. Evolution des tâches

Depuis l'entrée en vigueur de la LPD, le nombre des recours et des demandes de conseil n'a fait qu'augmenter. Les questions relatives au droit de la protection des données suscitent un vif intérêt tant des organes fédéraux que de la part du secteur privé.
Les questions des organes fédéraux se concentrent, abstraction faite des questions spécifiques aux différents domaines, sur les conditions auxquelles une transmission de données personnelles est licite, et sur la déclaration des fichiers.

Le secteur privé, pour sa part, manifeste un intérêt marqué pour l'utilisation des données personnelles dans les relations de travail (gestion de dossiers du personnel, octroi de renseignements, etc.). De même, la question revient fréquemment de savoir quand un fichier doit être déclaré et quand il ne doit pas l'être, compte tenu de la "connaissance" qu'a la personne concernée de l'existence d'un tel fichier.
Un autre point d'intérêt général concerne l'obligation de déclarer les communications de données à l'étranger.
La demande fréquente de renseignements par téléphone de la part des services tant fédéraux que privés revêt un intérêt particulier. Dans la plupart des cas, il s'agit de questions relatives à l'interprétation de la loi, aux modalités du droit d'accès, à la déclaration et à l'enregistrement des fichiers, aux motifs justificatifs relatifs au traitement de données dans le secteur privé, à l'applicabilité de la loi dans les cantons, etc.

2. Information du public

Les travaux de relations publiques sont un des aspects essentiels de l'activité du PFPD. Les collaboratrices et collaborateurs du PFPD et le PFPD lui-même ont présenté à différentes manifestations des exposés traitant de la protection des données. Il est réjouissant de constater que ce thème suscite un vif intérêt. Malheureusement, compte tenu des faibles moyens en personnel dont nous disposons, il ne nous a pas été possible de participer à toutes les manifestations. Nonobstant cela, nous mettrons tout en oeuvre à l'avenir pour y assister le plus régulièrement possible.
Le 1er juillet 1993, le public a été informé au cours d'une conférence de presse de l'entrée en vigueur de la loi sur la protection des données.
Quelques mois plus tard, le 8 octobre 1993, notre Secrétariat organisait la première Conférence suisse des préposés à la protection des données. 29 représentantes et représentants de 19 autorités cantonales de protection des données y ont pris part, de même qu'un représentant de la Conférence suisse sur l'informatique, ainsi que le Secrétariat du PFPD. Après un aperçu de l'organisation du PFPD et une introduction à la LPD, les participants à la conférence ont eu l'occasion d'échanger leurs avis. Cette manifestation a mis en évidence l'utilité d'un échange d'expériences régulier et de la collaboration entre les autorités fédérales et cantonales. Les personnes présentes ont donc décidé d'institutionnaliser cette manifestation et de l'organiser chaque année afin de coordonner la protection des données sur l'ensemble de notre territoire.
Et enfin, le 4 mars 1994 a eu lieu la première séance d'information pour les organes de la Confédération. Ce fut là l'occasion d'un premier échange d'expériences entre les autorités fédérales et le PFPD.
Dans le cadre de notre activité d'information générale, nous avons élaboré quatre brochures sur le traitement des données personnelles: "Les droits de la personne concernée en matière de traitement de données personnelles", "Guide à l'usage des maîtres de fichiers", "Guide pour le traitement des données personnelles dans l'administration fédérale", et "Guide sur les mesures techniques et organisationnelles de protection des données". Les trois premières sont déjà publiées.
Par ailleurs, un commentaire à l'appui de l'ordonnance relative à la loi fédérale sur la protection des données a été établi.
D'autres brochures, aide-mémoire et guides seront publiés dans un proche avenir sur différents thèmes relatifs à la protection des données.

3. Dotation en personnel du Secrétariat du PFPD

Même si nous nous sommes efforçés de répondre le plus rapidement possible à toutes les questions des personnes privées et de l'administration, et de remplir les tâches légales précitées, nous n'avons pas réussi à accorder toute l'attention voulue à chacun des domaines d'activité. Au contraire, de nombreux retards se sont accumulés dûs à une surcharge de travail. Nous avons donc été contraints de fixer des priorités: le registre des fichiers, ainsi que nos activités de conseil et d'information constituent la première priorité.
Malgré ces mesures, force nous est de constater que sans augmentation de personnel, nous n'arriverons pas à accomplir toutes nos tâches de manière satisfaisante.

4. Formation et perfectionnement

Afin de transposer la protection des données dans la pratique, il faut avoir, outre une compréhension fondamentale de la matière, des connaissances spécialisées tant juridiques que technico-organisationnelles. En d'autres termes, la formation et le perfectionnement sont indispensables.
Les collaboratrices et collaborateurs du PFPD s'efforcent de couvrir jusque dans une certaine mesure les besoins fondamentaux inhérents à leur sphère d'activité. Il ne fait cependant aucun doute qu'il y a un important retard à combler, pour que nous soyons en mesure de trouver des solutions adéquates dans ce secteur complexe d'activités.

5. Statistique des activités du Préposé fédéral à la protection des données Période du 1er juillet 1993 au 30 mars 1994

Nombre de séances

Séances de travail	à l'extérieur	264
Participations à des conférences	nationales	12
	internationales	5

Nombre de prises de position

	Entrées	Pas de remarques	Pas d'objections	Conseil / prises de position écrites
Sur des lois	24		1	23
Sur des ordonnances	50	4	1	45
Sur des traités internationaux	26		4	22
Sur des questions du secteur privé	81	1		80
Sur des questions du secteur public	180	32		148

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:	2 personnes
Service de l'information:	Tsiraktsopulos Kosmas, lic. en droit
Chancellerie:	2 personnes