Préposé fédéral à la protection des données

Rapport d'activités 1997/98

Le Préposé fédéral à la protection des données est tenu de fournir périodiquement au Conseil fédéral un rapport sur son activité (article 30 de la loi fédérale sur la protection des données). Le présent rapport couvre la période du 1er avril 1997 au 31 mars 1998.

TABLE DES MATIÈRES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

AVANT PROPOS

Les dangers de la mise en réseau

Les réseaux de données, notamment aux travers des inforoutes, ne sont plus contrôlés uniquement par l'Etat. Les possibilités d'intervention étatique dans les nouvelles technologies de l'information qui permettent le traitement et la diffusion de données personnelles dans de vastes réseaux à l'échelle mondiale (par ex. Internet) sont de plus en plus limitées. Il est en effet difficile de connaître tous les acteurs de tels réseaux et de savoir quelles données y sont traitées, pour quelles finalités et à qui elles sont communiquées. Ainsi, je constate que nos lois, dont l'application est limitée au territoire national, ne sont pas toujours adaptées pour répondre au défi du «village global» et en particulier ne donnent pas les moyens de lutter efficacement contre les abus liés à la dissémination transfrontière des données. A nouveau, je me dois de rappeler que toutes activités nécessitant le traitement de données personnelles et en particulier au travers des réseaux, laissent des traces, qui peuvent un jour ou l'autre se retourner contre une personne, fut-elle innocente! Ces traces permettent de dresser des profils de la personnalité et remettent en cause le droit à la vie privée lors de communications internationales de données.

Face à cette évolution, j'estime que la protection des données ne peut plus être uniquement garantie par des lois nationales. Une réglementation internationale est nécessaire. En outre, le droit doit être relayé et complété par des normes techniques (technologie de la vie privée). Il faut ainsi rapidement développer une stratégie juridico-technique. Dans cette optique, je préconise notamment la mise à disposition des individus de moyens technologiques leur permettant de se protéger contre la tendance actuelle qui favorise les mécanismes disproportionnés de contrôle et de téléguidage. Dans une société informationnelle mondialisée, je demeure convaincu que le respect de la vie privée nécessite la garantie du droit à l'anonymat et à la confidentialité des communications pour toute personne se comportant conformément aux règles démocratiquement établies. Hélas aujourd'hui, je constate une tendance sécuritaire outrancière, dont l'efficacité n'est pas démontrée et qui pourrait remettre en cause l'équilibre démocratique.

Ainsi, la technologie doit également nous permettre de nous protéger et nous donner la possibilité de déterminer individuellement et selon les circonstances quelles données nous concernant peuvent être traitées (droit à l'autodétermination en matière d'information). Ces technologies sont aujourd'hui disponibles et permettent notamment de chiffrer nos messages. L'Etat a un rôle à jouer, non pas en freinant le développement de ces technologies, mais en encourageant leur développement. La liberté de communiquer dans le «village global» et le droit de bénéficier des avantages de la société d'information seront ainsi garantis si chaque individu a accès aux moyens techniques lui permettant de se protéger contre toute intrusion illicite et disproportionnée. Il est bien clair que le rôle régulateur de l'Etat ne doit pas se faire au détriment des règles du marché et de la concurrence. L'Etat se doit d'intervenir pour créer les conditions cadres permettant à l'individu de se protéger et de faire valoir ses droits.

L'avenir de la protection des données

Dans une société d'information, la protection des données est un élément indispensable de l'avenir de nos sociétés démocratiques. Je le pense non seulement pour garantir à l'individu son droit à la vie privée, mais également pour permettre à l'Etat d'accomplir ses tâches légales et de traiter des données personnelles lorsque cela est indispensable. Dans le secteur privé finalement, la protection des données peut contribuer à une gestion efficace des données. L'effectivité de la protection des données passe par un renforcement de la coopération internationale et l'adoption de textes internationaux de portée universelle. Elle nécessite en outre de plus en plus des développements techniques, sans qu'il soit nécessaire dans chaque cas d'espèce de créer des bases juridiques nouvelles. Des données personnelles ne peuvent être traitées pour l'accomplissement des tâches légales, le développement économique, le commerce ou encore la recherche que pour autant que cela soit nécessaire. Ainsi, je suis persuadé que de nombreuses tâches peuvent être réalisées sans recours à des données personnelles et c'est dans ce sens que doit continuer à oeuvrer la protection des données.

L'autonomie du Préposé fédéral à la protection des données

En tant que Préposé fédéral à la protection des données, je ne suis en mesure de remplir ma tâche que si mon autonomie, garantie par la loi, est respectée. Cela nécessite des moyens suffisants et un statut au bénéfice de compétences adaptées à l'ampleur de la tâche. Il est vrai que mes tâches de surveillance ne correspondent pas au schéma traditionnel d'une administration hiérarchiquement structurée. Bien que ma fonction soit respectée, je me heurte d'autre part aussi à l'ignorance, à l'incompréhension voire même aux suspicions. Je perçois au sein de l'administration des tendances à ignorer la protection des données au bénéfice de la rationalisation et des économies budgétaires. Or, celui qui traite des données ne doit pas oublier qu'il est lui-même sujet de traitements de données personnelles et au bénéfice des mêmes droits qu'il a tendance à contester aux autres!

Mon rôle n'est pas de freiner ou d'empêcher le développement de la société d'information et les traitements de données personnelles qui en découlent, dans la mesure où ils sont justifiés et nécessaires. Je dois cependant être le garant des intérêts multiples, qui concernent chacun d'entre-nous en tant qu'individu ou en tant que membre d'une société démocratique. Face à l'évolution technologique actuelle et au développement du «village global», il est difficile pour l'individu de reconnaître les menaces qui pèsent sur le respect de ses libertés. Trop souvent, l'individu n'est pas conscient des atteintes à sa vie privée et à ses droits fondamentaux ou il ne le remarque que bien après. Il n'est par conséquent pas toujours en mesure de faire valoir ses droits et de se défendre devant des appétits pas toujours légitimes en traitements de données personnelles. En d'autres mots: sans protection des données, il n'y a pas de démocratie et le respect des libertés et droits fondamentaux est remis en cause. Dès lors, dans l'intérêt bien compris de l'individu, l'autonomie du Préposé fédéral à la protection des données doit être garantie pour pouvoir continuer à contrôler les traitements de données personnelles effectués aussi bien dans le secteur privé que dans l'administration fédérale.

O. Guntern

REPERTOIRE DES ABREVIATIONS

ADMAS	Registre des mesures administratives
ADN (DNA)	Acide désoxyribonucléique
AFD	Administration fédérale des douanes
ASB	Association des banquiers suisses
AUPER	Système d'enregistrement automatisé des personnes
CFPD	Commission fédérale à la protection des données
CJ-PD	Groupe de projets sur la protection des données
Cond. gén.	Conditions générales
CP	Code pénal
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DOSIS	Système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants
EAV	Gestion électronique des dossier
GWG	Système de traitement des données en matière de lutte contre le blanchiment d'argent
InfV	Ordonnance sur les systèmes d'information et de paiement de l'assurance-chômage
IPAS	Système informatique de gestion et d'indexation des données et de personnes
ISIS	Système de traitement des données relatives à la protection de l'Etat
ISOK	Système de traitement des données en matière de lutte contre le crime organisé
JAAC	Jurisprudence des autorités administratives de la Confédération
LACI	Loi fédérale sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LBA	Loi fédérale relative à la lutte contre le blanchissage d'argent dans le secteur financier
LEg	Loi fédérale sur l'égalité entre femmes et hommes
LOC	Loi fédérale sur les offices centraux de police criminelle de la Confédération
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi sur la protection des données
LSEE	Loi fédérale sur le séjour et l'établissement des étrangers
LSF	Loi sur la statistique fédérale
MfG	Bureau de communication en matière de blanchiment d'argent
MOFIS	Système informatisé de véhicules à moteur
O-DOSIS	Ordonnance sur le système de traitement des données en matière de lutte contre le trafic illicite de stupéfiants
O-ISOK	Ordonnance sur le système de traitement des données en matière de lutte contre le crime organisé
OACI	Ordonnance sur l'assurance-chômage obligatoire et l'indemnité en cas d'insolvabilité
OAMal	Ordonnance sur l'assurance-maladie
OC stup	Office central de lutte contre le trafic illicite des stupéfiants

OCDE	Organisation de coopération et de développement économique
OFAS	Office fédérale des assurances sociales
OFDE	Office fédéral du développement économique et de l'emploi
OFE	Office fédéral des étrangers
OFP	Office fédéral de police
OFS	Office fédérale de la statistique
OM	Loi fédérale sur l'organisation militaire
ORen	Ordonnance sur le renseignement
ORI	Ordonnance du Tribunal fédéral sur la réalisation forcée des immeubles
PDA	Personnes, dossiers, antécédents
PLASTA	Ordonnance sur le système d'information en matière de placement et de statistique du marché du travail
RCE	Registre central des étrangers
RIPOL	Système de recherches informatisées de police
RNIS	Réseau numérique à intégration de services
SIG	Système d'information géographique *
StF	Loi fédérale sur le statut des fonctionnaires
VOSTRA	Casier judiciaire automatisé
ZAN	Index central des dossiers
Zent VO	Ordonnance sur les offices centraux de police criminelle
ZS OK	Office central de lutte contre le crime organisé
ZSD	Services des offices centraux

I. THEMES CHOISIS

1. Affaires de police

1.1. Création de bases légales pour des registres de personnes par l'Office fédéral de la police

Le 31 juin 1998, la période de transition prévue par la LPD pour que les organes fédéraux puissent créer les bases légales suffisantes pour les traitements existants de données sensibles et de profils de la personnalité arrive à son terme. Ayant subitement reconnu l'urgence de la situation, l'Office fédéral de la police (OFP) a soumis fin 1997 au Parlement pour examen un paquet de lois pour plusieurs registres de personnes. Le Conseil des Etats vient de proposer la prolongation de la période de transition jusqu'au 31 décembre 2000.

La LPD a prévu une période de transition de cinq ans à compter de son entrée en vigueur pour que les organes fédéraux puissent créer les bases légales suffisantes pour les traitements existants de données sensibles et de profils de la personnalité. Ayant subitement reconnu l'urgence de la situation, l'Office fédéral de la police (OFP) a élaboré un paquet de lois TGV, d'après le nom du fameux train à grande vitesse, afin de pouvoir légaliser ses traitements de données dans les délais. Ce paquet comprend des bases légales pour IPAS (Système informatisé de gestion et d'indexation des dossiers et des personnes), VOSTRA (Casier judiciaire automatisé), ADMAS (Registre des mesures administratives) et MOFIS (Registre des véhicules et détenteurs). En septembre 1997, le Conseil fédéral a publié le projet de loi ainsi que le message qui s'y rapporte et l'a soumis au Parlement. Le Parlement ne s'est pas senti en mesure de juger cette matière très complexe dans le temps très court qui restait jusqu'au 1er juillet 1998. C'est pourquoi la Commission juridique du Conseil des Etats a proposé avec une initiative parlementaire que l'on prolonge la période de transition de cinq ans par un arrêté fédéral jusqu'à fin 2000.

- IPAS

IPAS est une banque de données très complexe, qu'il est prévu d'utiliser comme système informatisé pour l'indexation et la gestion de personnes et de dossiers:

- IPAS devrait remplacer les systèmes AUPER-OFP (Système d'enregistrement automatisé des personnes) et ZAN (Index central des dossiers du Bureau central suisse de police).
- IPAS contiendra des données de base relatives à l'identité des personnes connues de l'OFP, ces données seront accessibles à tous les collaborateurs de l'OFP, en partie avec des renvois vers des systèmes d'information dans lesquels ces personnes sont enregistrées.
- IPAS contiendra un index des dossiers.
- IPAS devrait servir à diverses sections de l'OFP (identification, extradition, entraide judiciaire internationale, Interpol et police administrative) non seulement d'index automatisé des personnes et des dossiers mais aussi de système de gestion des dossiers. Dans le cadre de la gestion des dossiers, il sera possible de mémoriser dans le système des documents sous forme papier ou électronique.

- Pour les domaines susmentionnés, des données relatives à des cas seront en outre stockées dans IPAS.

Vu ces fonctionnalités très vastes, il est clair que le système IPAS contiendra des données sensibles. Il est prévu d'avoir des accès en ligne à IPAS pour le Ministère public de la Confédération pour effectuer des enquêtes de police judiciaire, ainsi que pour l'organe fédéral chargé, conformément à la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI), d'effectuer des contrôles de sûreté sur des personnes. Un accès en ligne à IPAS sera également consenti à l'organe fédéral qui, d'après la même loi, assiste les autorités de police et pénales compétentes en leur communiquant des constatations relatives au crime organisé, notamment dans le cas où de telles constatations sont faites dans le cadre de la collaboration avec des autorités de sécurité étrangères.
Alors que nous pouvons donner notre accord pour les accès en ligne des deux premières autorités, nous sommes d'avis qu'un tel accès consenti à l'autorité citée en dernier n'est ni conforme au principe de la proportionnalité, ni nécessaire pour l'accomplissement de la tâche mentionnée. Jusqu'à ce jour, l'autorité en question n'a pas été en mesure de démontrer que cette nécessité était plausible.
En ce qui concerne le renvoi prévu aux systèmes d'information qui traitent des données concernant la personne enregistrée, nous avons rendu attentif au fait que le renvoi à des systèmes d'information des Offices centraux de l'OFP violerait le principe de la séparation stipulé par la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération. Ce principe de la séparation statue que les systèmes d'information des Offices centraux de police criminelle doivent être exploités séparément d'autres systèmes d'information de la police et de l'administration. Cela signifie qu'il n'est pas permis d'inclure dans un système d'information de la police ou de l'administration des renvois à des données contenues dans les systèmes d'information des Offices centraux de police criminelle. Un tel renvoi impliquerait l'applicabilité du droit d'accès indirect prévu dans la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (voir aussi notre 4e rapport d'activités, p. 129). En biffant les systèmes d'information du projet, il n'existe plus à notre avis de justification juridique suffisante pour maintenir l'application du droit d'accès indirect. La désignation des services en tant que telle n'est à notre avis pas un traitement de données au sens de la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération, raison pour laquelle une application du droit d'accès indirect dans ce cas n'est pas justifiable.
Nous avons en outre rendu attentif au fait qu'aucun document des Offices centraux, que ce soit sous forme papier ou électronique, ne doit être mémorisé dans IPAS pour les raisons mentionnées plus haut et qui découlent du principe de la séparation.

- Fichiers de la loi sur la circulation routière (LCR)

(cf. Rapport d'activités 1995/96, p. 121)
Selon les informations fournies par l'Office fédéral de la police, les bases juridiques du registre des permis de conduire FA□ER ne seront pas établies dans le cadre de la révision „paquet TGV", mais en procédure ordinaire de révision de la LCR. L'ancrage de la réglementation relative au registre FABER dans une loi au sens formel est nécessaire, car des informations sensibles comme la nationalité ainsi que

des mesures administratives de police n'ayant pas encore force de chose jugée y sont traitées.
Dans le cadre de la consultation des offices, nous avons demandé que le registre des détenteurs de véhicules ne soit plus publié. Cette suppression se justifie d'autant plus que dans le projet de LCR, les autorités qui ont besoin de données sur les véhicules à moteur et leurs détenteurs auront désormais un accès en ligne à ces données.

- *Casier judiciaire entièrement automatisé VOSTRA*

Le projet de révision du code pénal prévoyait de garantir à la Police fédérale un accès illimité aux données VOSTRA (cf. Rapport d'activités 1996/97, p. 130). Nous avons demandé à l'occasion de la consultation des offices que l'accès en ligne de la Police fédérale à VOSTRA soit limité aux cas dans lesquels elle agit en tant que police judiciaire. Suite à un nouvel examen du projet de loi, nous avons constaté qu'un accès des organes de police à VOSTRA, même dans les limites que nous proposions, est illicite et doit donc être entièrement supprimé. Par ailleurs, nous avons proposé de n'autoriser que dans un volume limité l'accès des autorités fédérales compétentes aux données VOSTRA en vue d'effectuer les examens de sécurité relatifs à des personnes au sens de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure. Il convient en outre de supprimer la compétence du Conseil fédéral d'étendre l'accès à d'autres autorités lorsque le nombre des demandes de renseignement le justifie. La LPD requiert en effet que l'accès par procédure d'appel (en ligne) à des données sensibles soit expressément prévu par une loi au sens formel.

1.2. Ordonnance sur les Offices centraux

En même temps que l'ordonnance ISOK était élaborée, l'ordonnance d'exécution relative à la loi sur les Offices centraux de police criminelle de la Confédération fut mise en chantier.

Le 15 mars 1995, la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération entra en vigueur. Il fallut presque 3 ans pour qu'une ordonnance d'exécution pour cette loi soit mise en vigueur. Cette ordonnance ne s'applique cependant pas à tous les Offices centraux de police criminelle de la Confédération, mais seulement à ceux de l'Office fédéral de la police. L'élaboration de l'ordonnance fut démarrée en même temps que celle de l'ordonnance ISOK. Nous avons également été impliqués très tôt dans ce processus d'élaboration. Nos demandes ont été en partie acceptées. En ce qui concerne les différends subsistants, des accords ont finalement pu être trouvés.
A l'origine, nous nous étions opposés à l'intégration du Bureau central d'Interpol dans les Offices centraux. D'une part le Bureau central assume la fonction d'un prestataire de services neutre, sa tâche consistant à gérer la réception et la distribution au niveau national et international des demandes de renseignements relatives à la prévention et la poursuite de délits. Les demandes ne concernent donc pas seulement les domaines de la compétence des Offices centraux. D'autre part, les Offices centraux auraient connaissance de demandes qui ne sont pas de leur ressort. Conformément à la loi fédérale du 7 octobre 1994 sur les Offices centraux

de police criminelle de la Confédération, ces derniers ne sont autorisés à collecter des informations que si celles-ci sont nécessaires à l'accomplissement de leur tâche dans le cadre de cette loi. L'Office fédéral de la police nous a assuré par écrit que l'intégrité organisationnelle du Bureau central d'Interpol était garantie et que les collaborateurs des Offices centraux n'auraient pas connaissance d'informations dont ils n'ont pas absolument besoin pour l'accomplissement de leur tâche.
D'autre part, une obligation de rendre compte de la part des Offices centraux sous forme de rapport fut prévue pour l'activité d'analyse, pour laquelle il n'existe pas encore d'expériences. Ce rapport devrait informer sur la nature et le volume des données nécessaires pour l'analyse criminelle et faire des propositions pour définir des catégories de données.

1.3. Bureau de communication en matière de blanchiment d'argent

Pour lutter contre le blanchiment d'argent, un bureau de communication a entre autres été prévu dans la loi fédérale concernant la lutte contre le blanchiment d'argent (LBA). Avec l'entrée en vigueur de la LBA, ce bureau est opérationnel depuis le 1er avril 1998.

La loi fédérale concernant la lutte contre le blanchiment d'argent (LBA) prévoit la mise sur pied d'un bureau de communication en matière de blanchiment d'argent. Ce dernier dépend de l'Office central pour la lutte contre le crime organisé de l'Office fédéral de la police. La LBA est entrée en vigueur le 1er avril 1998 et le bureau de communication est également opérationnel depuis cette date. Ses tâches consistent entre autres à recueillir les renseignements de la part des intermédiaires financiers concernant les soupçons de blanchiment d'argent, d'examiner ces derniers, de procéder aux enquêtes nécessaires et le cas échéant d'informer les autorités pénales. Le bureau de communication dispose de 2 jours au moins, mais de 4 jours au maximum, pour s'acquitter de cette tâche. Pour être en mesure de remplir la mission que lui confie la loi, il a besoin de diverses informations en provenance de plusieurs banques de données policières. Ces informations sont des données sensibles au sens de la LPD. La contrainte du temps, l'effectif en personnel du bureau de communication ainsi que la fréquence de communication des données personnelles au bureau semblent rendre nécessaire une interrogation par des moyens de télécommunication ou même par procédure d'appel (liaison online). De telles communications de données nécessitent selon la LPD des bases légales sous forme d'une loi au sens formel. Nous sommes d'avis que la LBA n'a pas créé les bases légales formelles suffisantes pour de telles communications ou collectes de données. C'est pourquoi nous avons demandé au Conseil fédéral dans un rapport urgent, dans lequel nous avons exposé notre point de vue, de reporter l'entrée en vigueur de la LBA jusqu'à ce que les bases légales nécessaires soient créées. Ceci devrait éviter que le bureau de communication soit forcé, suite à l'omission de la part du législateur, de procéder à des traitements de données illicites. Vu les pressions politiques au niveau international, le Conseil fédéral estima ne pas pouvoir justifier un report de l'entrée en vigueur de la LBA. Nous avons alors donné notre accord pour une expérience pilote de 5 ans à condition qu'une ordonnance du Conseil fédéral règle les points suivants:

1. mention des banques de données dans lesquelles le bureau de communication consulte régulièrement des données sensibles par procédure d'appel ou par un autre moyen, l'énumération devant être restrictive;

2. limitation des données devant être communiquées au strict minimum nécessaire;
3. mention d'un catalogue des données détaillé;
4. liste des éventuelles autorisations d'accès;
5. limitation temporelle de la durée de validité de l'ordonnance applicable pour l'expérience pilote sans possibilité de prolongement;
6. obligation de rendre compte de la part du bureau de communication en matière de blanchiment d'argent après 2-3 ans d'activité sous forme d'un rapport écrit à l'intention du Préposé fédéral à la protection des données, renseignant sur les expériences qui ont été faites en ce qui concerne :

- la nécessité de communications régulières de données personnelles sensibles au bureau de communication par procédure d'appel ou par un autre moyen en provenance de banques de données;
- le volume des données à communiquer;
- les banques de données en provenance desquelles le bureau de communication nécessite des données personnelles pour accomplir sa tâche;

7. obligation de créer les bases légales correspondantes sur la base du rapport.

En même temps, l'Office fédéral de la police procédait à la consultation des offices pour une ordonnance du Conseil fédéral relative à une expérience pilote correspondante, à laquelle nous avons également été invités à prendre position.
La législation relative à la LBA est un exemple qui démontre clairement que de plus en plus souvent les travaux de législation ne tiennent pas compte des exigences formulées par la protection des données ou ne peuvent pas en tenir compte par manque d'expérience pratique. Dans des domaines complexes et importants, notamment en rapport avec le traitement de données sensibles et de profils de la personnalité, il y a lieu de recourir de plus en plus souvent à des expériences pilotes limitées dans le temps afin de pouvoir évaluer quelles données sensibles doivent être traitées, quel volume, par qui et pour combien de temps. De telles expériences pilote peuvent en outre éviter que des bases légales soient créées „pour le cas où" dans une loi au sens formel. Etant donné que la LPD prescrit toutefois que les bases légales nécessaires et suffisantes doivent exister avant que ne débutent les traitements de données, que les bases légales pour les expériences pilotes ne peuvent être décrétées que par voie d'ordonnance et pour une durée limitée, une question se pose: celle de l'opportunité d'accorder au Préposé fédéral à la protection des données la compétence d'approuver les expériences pilotes.

1.4. Droit d'accès conformément à la loi fédérale sur les Offices centraux de police criminelle de la Confédération

Au cours de l'année d'activité écoulée du Préposé fédéral à la protection des données, trois demandes de renseignements dans le domaine des Offices centraux de police criminelle de la Confédération ont été déposées.

Au cours de l'année écoulée, trois avocats nous ont contacté au nom de leur client et ont invoqué le droit d'accès conformément à la loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC).
Selon cette loi, toute personne peut demander au Préposé fédéral à la protection des données qu'il vérifie si des données la concernant sont traitées de manière licite auprès d'un Office central. Le préposé communique à la personne requérante par

une réponse standard selon laquelle aucune donnée la concernant n'est traitée de manière illicite ou que – dans les cas où une erreur de traitement existe – nous avons adressé une recommandation à l'Office central pour corriger cet état de fait. La lettre adressée par le préposé en réponse à la demande du requérant n'informe pas ce dernier si des données le concernant sont traitées par un Office central.
Dans un cas, nous étions parvenus à la conclusion que le droit d'accès n'était pas régi par la LOC, mais par la LPD, ce qui impliquait que nous n'étions pas l'organe compétent pour fournir ces renseignements. Le requérant s'adressa alors au maître du fichier qui lui refusa le droit d'accès en s'appuyant sur la LPD. Le demandeur fit alors recours contre cette décision auprès du Service des recours du Département fédéral de justice et police, où l'affaire est encore en cours, notamment à cause de la question de la compétence en matière de droit d'accès.

1.5. Système de traitement des données pour la lutte contre le crime organisé ISOK

La loi fédérale sur les Offices centraux de police criminelle de la Confédération prévoit que chaque office central de police criminelle de la Confédération peut gérer un système informatisé de traitement des données. Depuis le 1er janvier 1998, l'Office central pour la lutte contre le crime organisé dispose du système ISOK.

La loi fédérale sur les Offices centraux de police criminelle de la Confédération du 7 octobre 1994 (LOC) prévoit que chaque Office central de police criminelle de la Confédération au sens de la LOC peut exploiter un système informatisé de traitement des données pour l'accomplissement de ses tâches. C'est ainsi que l'Office central pour la lutte contre le crime organisé dispose depuis le 1er janvier 1998 – presque trois ans après l'entrée en vigueur de la LOC – du système informatique pour la lutte contre le crime organisé ISOK. ISOK est une banque de données sœur de celle utilisée pour la lutte contre le trafic illicite de stupéfiants.
La réalisation d'ISOK a été précédée par l'élaboration de l'ordonnance du Conseil fédéral du 19 novembre 1997 relative au système de traitement des données pour la lutte contre le crime organisé. Nous avons été impliqué de bonne heure dans ce processus d'élaboration. A part le fait que nous sommes d'avis que les données stockées dans le système et désignées comme données appartenant à la police judiciaire/données n'appartenant pas à la police judiciaire doivent être séparées logiquement par des autorisations d'accès distinctes (voir à ce propos le 4e rapport d'activités, p. 128), toutes nos demandes ont été reprises dans l'ordonnance.

1.6. Commission d'experts pour une banque de données suisse des profils d'ADN dans le domaine policier

Lors de délits, des analyses comparatives de traces de sperme, de peau ou de cheveux trouvées sur les lieux de l'infraction ainsi que d'échantillons de sang ou de salive prélevés sur des suspects peuvent mener à l'identification des coupables. De telles méthodes comparatives étant utilisées de plus en plus souvent par les cantons, la question d'une banque de données suisse de profils d'ADN a été soulevée.

Une analyse de traces de sperme, de peau ou de cheveux trouvées sur les lieux de l'infraction permet d'identifier sans équivoque les coupables au cas où ces traces sont comparées avec des échantillons de sang ou de salive prélevés sur des

personnes suspectes, et que les coupables se trouvent parmi les suspects. Comme une telle analyse permet avec une probabilité avoisinant les 100 % d'identifier les vrais coupables ou de disculper des personnes suspectées à tort, les analyses d'ADN deviennent de plus en plus populaires dans les milieux policiers. De gros problèmes apparaissent cependant en rapport avec le prélèvement des échantillons de salive ou de sang sur les personnes suspectes, l'analyse et la conservation de ces derniers, la mise en relation des résultats avec les données personnelles, l'effacement, la transmission, les aspects de l'efficacité du travail policier et de la lutte contre le crime, etc. Se pose entre autres la question de la création d'une banque de données nationale de profils d'ADN. Le 25 novembre 1997, le Département fédéral de justice et police a constitué une commission d'experts chargée d'examiner s'il y a lieu de mettre sur pied une telle banque de données, si une telle opération est justifiée et opportune, comment une telle banque de données doit être structurée et légitimée sur le plan légal. Cette commission d'experts, dans laquelle siège également le Préposé fédéral à la protection des données, s'est réunie pour sa séance constitutive en janvier 1998.

1.7. Ordonnance sur le Service de surveillance de la correspondance postale et des télécommunications

Dans le cadre de la libéralisation du marché des télécommunications, il devint nécessaire que les surveillances téléphoniques ordonnées ne soient plus effectuées par les PTT. A cette fin, on a mis sur pied par voie d'ordonnance un service qui, depuis le 1er janvier 1998, effectue les surveillances téléphonique en collaboration avec les divers fournisseurs.

Jusqu'à fin 1997, les surveillances téléphoniques ordonnées à des fins de poursuite et de prévention d'actes délictueux étaient exécutées par les soins des PTT. Depuis le 1er janvier 1998, le marché des télécommunications est libéralisé. Cela signifie qu'il va y avoir sur ce marché plusieurs entreprises offrant des prestations dans le domaine des télécommunications et qui entreront en concurrence avec l'ancienne entreprise des PTT. Il serait choquant que les surveillances téléphoniques ordonnées soient encore exécutées par les PTT, ce qui impliquerait que ces derniers les effectuent même auprès de leurs concurrents. C'est la raison pour laquelle on a créé – par voie d'ordonnance du Conseil fédéral du 1er décembre 1997 sur le Service de surveillance de la correspondance postale et des télécommunications – un service, dépendant sur le plan administratif du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC). Ce service effectue les surveillances téléphoniques en collaboration avec les divers fournisseurs.
Nous avons eu la possibilité de prendre position par écrit sur le projet d'ordonnance.

2. Droit des étrangers et droit d'asile

2.1. Objection contre les accès des organes de police aux fichiers du DFJP sur les requérants d'asile et les étrangers – divergences de droits dans un domaine délicat

Suite à la décision du Tribunal fédéral, il est devenu clair que le Préposé fédéral est limité au rôle d'observateur lorsqu'un département refuse sa recommandation en matière de protection des données. Cet état de fait est très insatisfaisant, en particulier dans les cas critiques et souvent très complexes de protection des données. Ce sont des cas où le citoyen est dépassé et la protection des données menacée de dépendre uniquement de la convenance des autorités (de police). Une motion en cours offre à présent la possibilité de corriger la LPD en ce qui concerne cette question.

Suite à notre recours, la Commission fédérale de la protection des données (CFPD) a annulé deux décisions du DFJP (cf. rapport d'activité 1996/97: p. 131). Ces décisions permettaient à l'Office fédéral de la police d'effectuer des accès en ligne aux fichiers de la Confédération concernant les requérants d'asile et les étrangers. Nous avions défendu le point de vue que seul un nombre très restreint de ces accès étaient admissibles, et ce uniquement après que les bases légales nécessaires aient été créées et que toutes les questions importantes relatives à la sécurité aient été résolues. La CFPD a en substance appuyé notre point de vue. Au lieu de mener enfin à bout l'analyse d'opportunité et de sécurité dont la CFPD l'avait chargé, le DFJP a déposé un recours contre la décision de la CFPD auprès du Tribunal fédéral. Le DFJP se réfère aux matériaux relatifs à la loi sur la protection des données et démontre que le Parlement n'était pas enclin – contrairement à la demande du Conseil fédéral – à consentir au PFPD un droit de recours contre les décisions d'un département. Le Tribunal fédéral examina la question en détail dans son arrêt. A cette occasion, il étudia soigneusement les considérants avancés par la CFPD pour affirmer sa compétence dans le cas concret. La CFPD avait argué que le PFPD devait au moins avoir un droit de recours dans les cas où il se trouvait gravement entravé dans l'accomplissement des tâches qui lui étaient confiées par la loi. Elle avait considéré cette condition comme remplie. Le Tribunal fédéral conclut cependant que le législateur n'avait pas opéré une telle distinction. Il n'examina donc pas non plus si et le cas échéant dans quelle mesure le PFPD avait été entravé dans l'exécution de ses tâches dans le cas présent. Il retint que le PFPD avait bien un statut autonome au sein de l'administration, mais qu'il n'avait donc pas – selon la volonté du législateur – de droit de recours. C'est la raison pour laquelle la CFPD n'aurait pas eu le droit d'examiner son recours. Le Tribunal fédéral annula ainsi la décision de la CFPD.
Cette question de droit ayant été tirée au clair, toute une série de questions matérielles se posent. Dans le cas concret, deux autorités de protection des données indépendantes ont l'une après l'autre – et en toute concordance – constaté une violation des dispositions de protection des données et demandé que celle-ci cesse. Les deux autorités de protection des données ont abouti à cette conclusion après avoir effectué des enquêtes relativement laborieuses, en particulier concernant des aspects techniques que le citoyen ou la personne concernée n'est pas en mesure de percevoir et qui sont en outre très complexes. A notre avis, il n'est pas satisfaisant, en particulier dans les cas critiques, qu'après un refus de la part d'un département, notre recommandation soit tout simplement écartée. C'est surtout dans les cas critiques que les problèmes de protection des données qui ont été

constatés doivent être examinés très soigneusement afin d'y trouver une solution irréprochable dans un état de droit. Le régime actuel contient à notre avis une grave lacune au niveau de la protection juridique. Il peut être opportun de laisser le citoyen décider s'il désire faire usage de son droit d'accès ou non. Une telle question ne nécessite pas l'intervention du PFPD. Par contre, lorsqu'une erreur de système intervient lors d'un traitement de données au sein d'une autorité, le citoyen qui en est touché ne sera vraisemblablement pas en mesure de constater ceci lui-même. S'il attend de la part de l'autorité en question qu'elle prenne une décision positive dans une affaire importante pour lui, il se gardera bien de troubler la bonne entente en objectant contre la protection des données.
Nous sommes donc d'avis qu'il existe une lacune importante dans le système de protection juridique de la loi sur la protection des données. Cette lacune devrait être comblée aussi rapidement que possible, si possible dans le sens qu'avait proposé en son temps le Conseil fédéral et le PFPD devrait être autorisé à faire examiner par la Commission fédérale de la protection des données le rejet de ses recommandations par un département. La motion déposée par Madame la Conseillère nationale von Felten donne désormais la possibilité de rectifier la LPD en ce qui concerne cette question très importante. Dans le cadre de la consultation des offices, nous avons soutenu cette motion et avons demandé au Conseil fédéral de l'accepter.

2.2. Délivrance électronique de visas en Suisse et à l'étranger; du projet informatique à la disposition légale

Les visas d'entrée en Suisse pourront bientôt être délivrés de manière électronique. Le projet informatique traverse la phase décisive du contrôle de sécurité. Conformément à la loi sur la protection des données, les bases légales ont également été adaptées.

Le projet informatique « délivrance automatisée de visas », sur lequel nous avions déjà informé en détail (4e rapport d'activité 96/97, p. 132) a traversé la phase de conception et se trouve peu avant sa réalisation. Il permettra aux représentations suisses à l'étranger et aux postes frontières – dans les cas ne posant pas de problèmes particuliers – de délivrer immédiatement les visas nécessaires pour une entrée en Suisse. Les données concernant les visas sont mémorisées dans un fichier spécial du Registre central des étrangers. Avant de délivrer une autorisation d'entrée, le Registre central des étrangers est consulté ainsi que si nécessaire le registre des recherches RIPOL et le fichier AUPER contenant les données des requérants d'asile. Les représentations à l'étranger n'accèdent cependant pas en mode online aux données sensibles; c'est plutôt le système qui procède aux contrôles nécessaires en Suisse pour ensuite ne transmettre que le résultat sous forme sommaire. Ceci mène à une réduction considérable des transferts de données et en même temps des questions relatives à la sécurité ainsi que nous l'avions demandé lors de l'analyse préliminaire. Actuellement, les spécialistes de la Confédération procèdent à l'analyse de sécurité encore en suspens dans laquelle ils impliquent également les utilisateurs à l'étranger. Vu le nombre élevé d'utilisateurs et les différents niveaux de compétence auxquels nous sommes confrontés, il est primordial dans ce cas de coordonner les aspects de sécurité. Nous avions insisté sur ce fait dans la phase de conception. Le concept de sécurité qui nous avait été présenté à l'époque avait laissé d'importantes questions en suspens. Le rapport de sécurité que nous attendons avec intérêt n'est pas encore disponible.

Pour pouvoir effectuer les traitements de données poussés, en partie nouveaux, qui sont nécessaires pour la délivrance d'un visa, il a été nécessaire d'adapter les bases légales existantes. Etant donné que le fichier des visas contient des données personnelles sensibles et que la consultation a lieu par procédure d'appel, des dispositions à cet égard ont dû être intégrées à la loi sur le séjour et l'établissement des étrangers. Ceci a eu lieu dans le cadre de la révision en cours de cette dernière. Quant à la délivrance des visas, elle fait l'objet d'une propre ordonnance qui remplace les anciennes normes surannées datant des années 40. Les dispositions techniques et la description du catalogue des visas ont été intégrées dans l'ordonnance sur le RCE. Avec l'entrée en vigueur des ces dispositions et à condition que le rapport de sécurité débouche sur un résultat positif, le système pourra être mis en service.

2.3. Sécurité informatique lors de la collaboration entre les autorités de police des étrangers de la Confédération et des cantons

Avec l'informatisation croissante de la coopération, l'aspect de la sécurité revêt une importance de plus en plus grande. Les données de la Confédération ne doivent pas être soutirées depuis un système informatique cantonal pour des utilisations à des fins contraires. Les données sensibles doivent être cryptées et leur traitement doit être journalisé.

Dans une affaire à caractère plutôt spectaculaire pour les initiés de la protection des données, une collaboratrice d'une autorité de police des étrangers d'un canton avait réussi pendant un certain temps à falsifier des livrets pour étrangers. Le hasard a voulu qu'un de ces livrets falsifiés a pu être confisqué sur la personne d'un trafiquant de drogue qui l'avait utilisé pour justifier de manière frauduleuse sa présence en Suisse. La contrefaçon avait été rendue possible par des manipulations non contrôlées de la collaboratrice mentionnée au niveau du registre central des étrangers (RCE) et dans le système informatique du canton en question. En collaboration avec le délégué à la protection des données du canton concerné, nous avons fait procéder à une enquête qui à ce jour n'est pas encore achevée. Au niveau de la Confédération, nous avons en outre demandé que l'Office fédéral des étrangers et le centre de calcul du DFJP procèdent à une analyse des risques et fournissent un rapport de sécurité sur le RCE, ainsi que nous l'avions déjà demandé – malheureusement sans succès – avec notre recommandation relative au RCE à l'intention du DFJP et de notre recours subséquent auprès de la Commission fédérale de la protection des données (CFPD) (cf. 3e rapport d'activités 1995/96 p. 122). En même temps, nous avons demandé à la CFPD des mesures préventives pour améliorer la sécurité au sein du RCE. Sur ce, la CFPD a statué que les accès online au RCE devaient être journalisés avec effet immédiat et que les données du RCE devaient être cryptées. Selon un communiqué du DFJP, ces mesures ont entre-temps été appliquées, ce qui signifie que nous serons en mesure après réception du rapport de sécurité d'examiner leur aptitude ainsi que celle des autres aspects de sécurité.
Nous espérons que ce cas de contrefaçon reste un cas unique en Suisse. Il est absolument nécessaire que la Confédération et les cantons collaborent étroitement en ce qui concerne la sécurité, comme nous l'avions déjà demandé précédemment avec insistance (cf. 4e rapport d'activité 1996/97, p. 133). Cela signifie que les cantons doivent éventuellement renoncer à certains désirs de traitement de données

au cas où ces désirs risqueraient de créer une situation dans laquelle la sécurité ne pourrait plus être financée (cf. notre avis dans JAAC 60.10). D'autre part, les cantons devraient adapter les moyens informatiques qu'ils utilisent pour traiter des « données de la Confédération » aux normes de sécurité qui sont nécessaires dans de tels cas, même s'ils ont saisi ces données eux-mêmes. C'est le seul moyen de garantir une sécurité des données légalement suffisante sur l'ensemble du pays. Bien que ceci soit plus largement compris, ce n'est malheureusement pas encore le cas partout.

2.4. A propos des limites de l'autonomie cantonale en matière de mise en oeuvre du droit des étrangers (exemple de l'entraide administrative)

Les cantons agissent de manière autonome par rapport au droit fédéral en ce qui concerne l'organisation des dispositions d'exécution. Ils doivent néanmoins respecter les exigences du droit fédéral. Cela signifie que l'entraide administrative intercantonale doit être conçue d'une manière conforme au droit fédéral. Une loi cantonale d'application pour la LSEE s'appuiera donc de préférence très étroitement aux dispositions sectorielles en matière d'entraide administrative du droit fédéral.

Le droit des étrangers de la Confédération oblige les autorités de la Confédération et des cantons dans nombre de cas à s'aider mutuellement. Les autorités de police des étrangers des cantons doivent être informées lorsque des circonstances se produisent qui pourraient avoir une incidence sur l'autorisation de séjourner d'un étranger en Suisse. Un tel cas se produit par exemple lorsqu'un étranger est condamné à une peine importante ou si le divorce pour un mariage avec un citoyen ou une citoyenne suisse est prononcé peu de temps après la date du mariage. Les tribunaux cantonaux sont donc tenus de communiquer d'eux-mêmes à la police cantonale des étrangers de manière appropriée les jugements pénaux importants et les jugements de divorce concernant des étrangers. En règle générale, une communication des dispositifs du jugement devrait suffire. Les communications qui ne sont pas absolument nécessaires pour le règlement des questions relatives au droit des étrangers ne doivent pas avoir lieu. En règle générale, la police des étrangers n'a pas besoin des considérants détaillés des jugements ou des dossiers (de divorce) proprement dits.
Dans un avis publié dans la JAAC 62.20, nous avons exprimé notre position sur cette question ainsi que sur d'autres questions similaires. Nous y avons abouti à la conclusion que le projet d'une disposition d'entraide administrative pour une loi cantonale d'application sur la LSEE qui nous avait été présentée avait été conçue de manière un peu exagérée. La disposition en question demandait ni plus ni moins la communication de tous les jugements et procédures concernant des étrangers à la police des étrangers. Ceci mènerait vraisemblablement à un volume de communication de données dépassant ce que le législateur souhaite et qui en outre ne serait pas couvert par le droit fédéral. A notre avis, il suffit que les tribunaux communiquent à la police des étrangers les faits qu'ils jugent importants après avoir procédé eux-mêmes à une première sélection raisonnable.

2.5. A propos de la sécurité du „compte de sécurité“ pour requérants d'asile auprès de la Poste et du rapport de sécurité de l'Office fédéral des réfugiés

Pas de protection efficace des données sans sécurité. C'est surtout pour les traitements de données extrêmement délicats dans le domaine de l'asile que de

bonnes mesures de sécurité s'imposent. Après de longs et vastes travaux, l'Office fédéral des réfugiés a élaboré un rapport de sécurité incluant un catalogue de mesures pour ses propres traitements de données, rapport qui sera présenté sous peu. Ce qui compte, c'est que les mesures de sécurité des données soient appliquées aussi bien dans les services que dans les centres de calculs (exploitant du centre de calcul).

L'Office fédéral des réfugiés et la Poste gèrent en coopération des „comptes de sécurité" des requérants d'asile. Sur la base de notre recommandation du 30 janvier 1995 (voir aussi rapport d'activité 1995/96, p. 128), l'Office fédéral des réfugiés et la Poste se sont engagés à améliorer la sécurité des données de ces comptes. La nouvelle solution prévoit entre autres l'utilisation de procédés de cryptage et de cartes à puce. Il est prévu par la suite de faire certifier le nouveau système.
Dès la fin de 1994, l'Office fédéral des réfugiés commença en outre à procéder à une vérification systématique de la sécurité des données au sein de l'office. En collaboration avec des spécialistes de la sécurité de l'Office fédéral de l'informatique et de l'université de Zurich on procéda à un inventaire des objets à protéger et on élabora un catalogue de mesures. Nous avons donné un avis positif concernant le rapport intermédiaire présenté en 1996 tout en mentionnant quelques points posant problème. La condition indispensable pour garantir une sécurité des données qui soit bonne et exempte de failles est qu'il y ait une bonne collaboration entre les services et les centres de calculs (exploitants de l'informatique).

2.6. Le changement de nom selon le CC doit également être appliqué pour les étrangers

Lorsqu'un étranger change son nom conformément aux dispositions du Code civil (CC), le nouveau nom doit dès lors figurer sur son livret pour étrangers ainsi que dans le registre des étrangers. L'ancien nom ne doit plus être accessible qu'à un nombre très restreint de personnes autorisées. Il n'est pas permis de continuer à utiliser l'ancien nom dans les relations avec les autorités ou même à des fins publicitaires privées. L'étranger peut demander un blocage ou une rectification.

Par décision du gouvernement, un étranger avait obtenu sur la base de l'article 30, 2ème alinéa CC le droit d'utiliser dorénavant le nom de son épouse. Son ancien nom, qu'il avait donc déposé, continua cependant à figurer dans son livret pour étrangers ainsi que dans le registre des étrangers. Même Swisscom continua à lui adresser le courrier publicitaire à son ancien nom. L'étranger demanda sans succès aux autorités compétentes de n'utiliser que son nom légal pour le courrier officiel et privé. Le cas nous a été soumis par le préposé bernois à la protection des données pour examen du point de vue du droit fédéral en matière de protection des données. Nous avons demandé un avis de droit à l'Office de l'état civil (Office fédéral de la justice) sur les implications d'un changement de nom dans les relations officielles et privées. Selon cet avis, seul le nom légal, donc le nouveau nom, peut être utilisé après le changement de nom. Si ce nom se compose uniquement du nom du conjoint, seul ce nom peut être utilisé. Des exceptions peuvent être faites pour des personnes qui peuvent prouver un intérêt particulier à connaître l'ancien nom ou pour des personnes du registre qui doivent également connaître l'ancien nom. Ainsi, selon la loi sur la protection des données, le nom «correct» est également le nom légal que le porteur désire utiliser. L'ancien nom ne peut donc par principe plus être utilisé pour les relations officielles et privées, donc à défaut d'une disposition contraire

explicite même pas sur le livret pour étrangers ou dans les rubriques du registre des étrangers qui peuvent être rendues accessibles à un grand nombre de personnes.

2.7. Exigences en matière de protection des données lors de la collecte de données concernant des étrangers et des requérants d'asile à des fins de recherche

La collecte de données concernant des étrangers et des requérants d'asile à des fins de recherche nécessite une bonne protection des données. Les données recueillies doivent être rendues anonymes aussi rapidement que possible. Les données qui pourraient permettre d'identifier certaines personnes doivent être gardées sous clé et doivent être complètement séparées des autres fichiers. Les accès doivent être surveillés. Les données sensibles doivent être cryptées.

Dans le cadre de projets de recherche nationaux ou autres on procède de plus en plus souvent à la collecte de données extrêmement sensibles concernant des étrangers et des requérants d'asile. Une bonne intégration des étrangers est un objectif important de la politique suisse envers les étrangers. Celle-ci entraîne donc une grande responsabilité quant au traitement correct des données qui sont recueillies à cette occasion. Les renvois vers des personnes identifiables ne doivent être conservés que pour la durée qui est absolument nécessaire. Les données personnelles doivent être gardées sous clé. Au cas où elles sont traitées par des moyens informatiques, ce qui de nos jours risque d'être la norme, elles doivent être strictement séparées d'autres fichiers ou traitements de données et protégées efficacement contre les accès non autorisés. Des données extrêmement sensibles telles que par exemple des informations relatives à l'état de santé de personnes identifiables ou l'appartenance à une ethnie différente relativement bien définie, devraient uniquement être conservées sous forme cryptée. Les accès à de telles données ne doivent être concédés qu'à un cercle de personne très restreint et doivent en plus être contrôlés par le système (journalisation). L'Office fédéral des étrangers a élaboré un contrat standard pour les organes de recherche qui ont besoin de données en provenance du registre central des étrangers. Nous saluons une telle mesure. Elle permet en outre de définir le cadre de la protection des données dans la recherche de manière coopérative et de surveiller son application conjointement avec les chercheurs.

2.8. Protection des données dans la loi révisée sur l'asile et sur les étrangers – sujet incontesté au Conseil des Etats

Après le Conseil national, le Conseil des Etats a également approuvé les dispositions de protection des données dans la loi sur l'asile et dans la LSEE. Ainsi, les bases légales nécessaires selon la loi sur la protection des données pour les fichiers et les traitements de données sensibles dans le domaine du droit d'asile et des étrangers ont été créées. Relevons le fait réjouissant que le Conseil des Etats a accepté nos propositions d'amendement. De manière générale, on peut dire que de bonnes solutions ont été trouvées pour une matière très complexe.

Un complément important et nécessaire a pu être introduit avec une disposition relative à la délivrance automatisée des visas (cf. p. 133 du présent rapport ainsi que 4e rapport d'activités 1996/97, p. 132). En outre, la norme de délégation qui octroie

au Conseil fédéral la compétence de signer des accords importants entre Etats a été précisée. Les accès online aux fichiers sensibles des requérants d'asile et des étrangers sont en outre uniquement concédés aux autorités explicitement mentionnées et uniquement dans les cas où ceci est absolument nécessaire pour l'accomplissement d'une tâche assignée par la loi. De plus, on renoncera à saisir sans exception les empreintes digitales de tous les requérants d'asile. D'une manière générale, on peut qualifier cet arsenal législatif d'équilibré pour un domaine aussi délicat que complexe. A en juger du cours qu'ont pris les délibérations jusqu'ici, nous nous attendons à ce que le bon niveau de protection des données reste également incontesté au cours de la prochaine phase.

3. Télécommunications

3.1. Nouveau droit des télécommunications

L'entrée en vigueur au 1er janvier 1998 de la loi sur les télécommunications et de ses ordonnances d'application a entraîné un certain nombre de nouveautés pour les usagers. Ils peuvent obtenir une facture détaillée et n'ont plus l'obligation de figurer dans l'annuaire téléphonique.

En matière de relevés de taxes détaillés, nous avions défendu le maintien de la solution de l'ancienne loi, à savoir la communication des indicatifs des centraux locaux (par ex. 033 333 xx xx). Le législateur a préféré la solution de la communication de la totalité du numéro appelé (par ex. 033 333 33 33). Le nouveau droit des télécommunications ne contient pas de dispositions conciliant les droits des abonnés recevant des factures détaillées avec le droit à la vie privée des utilisateurs appelants et des abonnés appelés. Il n'est de ce fait pas compatible avec la directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Depuis l'entrée en vigueur du nouveau droit des télécommunications au 1er janvier 1998, l'abonné peut donc exiger de son fournisseur de services de télécommunication qu'il lui communique les données suivantes: les ressources d'adressage des raccordements appelés, c'est-à-dire les paramètres de communication (les éléments permettant d'identifier les personnes, les processus informatiques, les machines, les appareils ou les installations de télécommunication qui interviennent dans une opération de télécommunication) ainsi que les éléments de numérotation tels que les indicatifs, les numéros d'appel et les numéros courts; la date, l'heure et la durée des communications ainsi que la rémunération due pour chaque communication.
Depuis le début de l'année, l'abonné n'a également plus l'obligation de figurer dans un annuaire téléphonique (électronique ou sous forme papier). Il a également le choix entre plusieurs possibilités de rendre accessibles au public ses coordonnées téléphoniques. L'abonné qui opte pour la possibilité de ne figurer dans aucun annuaire ne court aucun risque en cas d'appel d'urgence. La loi sur les télécommunications stipule que le fournisseur de services de télécommunication doit organiser l'accès aux services d'appels d'urgence de sorte que les appels puissent être localisés. L'ordonnance sur les services de télécommunication précise que la localisation doit également être garantie pour les abonnés qui ont choisi de ne pas s'inscrire dans un annuaire.

- *L'exemple de Swisscom*

Swisscom offre à ses abonnés plusieurs possibilités de rendre accessibles au public les coordonnées téléphoniques (listes „blanche", „verte", „rouge" et „noire"). L'abonné „blanc" figure avec son numéro de téléphone et son adresse dans tous les annuaires disponibles (annuaire sur papier ou électronique, service de renseignement 111, CD-ROM etc.). L'abonné „vert" n'est pas inscrit dans les annuaires sur papier et sur CD-ROM. Il figure dans l'annuaire électronique et ses coordonnées sont disponibles au service de renseignements 111. L'abonné „rouge" dispose des mêmes choix que l'abonné „vert", mais cette liste n'indique que son adresse. En cas de recherche, Swisscom se contente de confirmer l'inscription de l'adresse. Le numéro de téléphone n'est en revanche pas accessible. L'abonné „noir" ne figure nulle part. Nous tenons ici à rappeler que ceux qui optent pour la liste „noire" ou pour la liste „rouge" ne courent aucun risque en cas d'appel d'urgence.

3.2. Règles de protection des données applicables aux concessionnaires du service universel

En matière de télécommunications, les concessionnaires du service universel sont, en tant que personnes privées accomplissant une tâche de la Confédération, soumises aux dispositions de protection des données applicables aux organes fédéraux.

Avec la libéralisation du marché des télécommunications et la privatisation de Télécom PTT devenu Swisscom, plusieurs questions liées au statut de cette entreprise sous l'angle de la protection des données nous ont été soumises. En effet, les règles concernant l'exigence d'une base légale, la surveillance, le contrôle et l'obligation d'annoncer les fichiers ne sont pas identiques pour un organe fédéral que pour une personne privée. Dans les domaines ne relevant pas du service universel, la situation est claire: les fournisseurs de services de télécommunication sont des personnes privées en concurrence économique entre elles, soumises aux dispositions de protection des données applicables aux personnes privées. Par contre, les concessionnaires du service universel, bien qu'étant également des personnes privées, accomplissent une tâche de la Confédération définie dans la loi sur les télécommunications et sont donc soumis aux dispositions de protection des données régissant les organes fédéraux. Un certain nombre de problèmes va surgir, notamment du fait que les concessionnaires du service universel seront également concessionnaires d'autres services. La distinction, par exemple, entre fichiers contenant des données sur les abonnés du service universel et ceux concernant les clients d'autres services pourrait se révéler difficile. Des solutions pratiques devront être trouvées avec les différents acteurs en présence: les fournisseurs de services de télécommunications, en particulier le ou les concessionnaires du service universel (Swisscom a obtenu une telle concession jusqu'en 2002), l'Office fédéral de la communication et l'Office fédéral de la justice.

3.3. Droit d'accès et communication à l'abonné de données relatives à la facturation

Les dispositions régissant la communication à l'abonné de données relatives à la facturation ne restreignent pas le droit d'accès.

L'Office fédéral de la communication, se basant sur un avis de droit sommaire émanant du Secrétariat général du DFJP, soutient le point de vue que la loi sur les télécommunications et ses ordonnances d'application permettent une restriction du droit d'accès et a informé Swisscom qu'il devait refuser toutes les demandes d'accès. Nous ne partageons pas ce point de vue.
Le droit d'accès est un droit fondamental pour la personne concernée et l'institution-clé de la protection des données. Ce n'est qu'ainsi que l'intéressé pourra faire valoir ses droits, en particulier faire rectifier des données inexactes, en contester l'exactitude ou les faire le cas échéant détruire. Ce droit a en outre un effet préventif certain. Même si les particuliers en feront rarement usage, le seul fait, pour le maître d'un fichier, de connaître l'existence de ce droit l'incitera à traiter correctement les seules données personnelles dont il aura vraiment besoin. Afin que ce droit puisse être exercé par chacun, indépendamment de sa situation financière, le législateur a prévu le principe de la gratuité du droit d'accès. Une participation aux frais peut exceptionnellement être demandée par le maître du fichier lorsque le droit d'accès a déjà été exercé dans les 12 mois précédant la demande sans modification non annoncée des données relatives à l'intéressé. Idem si la communication des renseignements demandés occasionne un volume de travail considérable. Le maître de fichier peut en outre refuser ou restreindre la communication des renseignements demandés si une loi le prévoit, les intérêts prépondérants d'un tiers l'exigent, un intérêt public prépondérant le requiert notamment en matière de sûreté intérieure ou extérieure de la Confédération (valable uniquement pour un maître de fichier public), le déroulement d'une procédure d'instruction risque d'être compromis (valable uniquement pour un maître de fichier public) ou ses propres intérêts prépondérants le requièrent (valable uniquement pour un maître de fichier privé). Encore faut-il que les données ne soient pas communiquées à des tiers. Le droit d'accès et la communication à l'abonné de données relatives à la facturation poursuivent des buts différents. Le premier permet à la personne concernée d'exercer un „contrôle" sur la totalité des données traitées par son fournisseur de services de télécommunication alors que la seconde donne à l'abonné la possibilité de vérifier les factures établies par son fournisseur de services de télécommunication. Il est donc logique qu'une disposition légale ne peut restreindre l'application d'une autre norme couvrant un domaine différent. De plus, sans entrer dans les détails juridiques, seule une loi au sens formel permet de restreindre ou refuser le droit d'accès, et la loi sur les télécommunications ne contient aucune disposition de ce genre.

3.4. Affichage et suppression de l'affichage des numéros d'appel

La controverse qui règne concernant la perception d'une taxe pour la mise en place du blocage du numéro de l'appelant n'a pas encore pu être entièrement réglée. La décision du Département fédéral des transports, des communications et de l'énergie (DFTCE, aujourd'hui DETEC) de mars 1997, selon laquelle une telle taxe peut continuer à être perçue, a été contestée par des clients de Swisscom devant la Commission fédérale de la protection des données.

Le thème de l'affichage et de la suppression de l'affichage du numéro de l'appelant nous occupe depuis plusieurs années déjà (voir également notre 4e rapport d'activité, p. 138). Dans un réseau numérique à intégration de services (RNIS) ainsi

que dans le réseau numérique de téléphonie mobile (NATEL D), les personnes recevant un appel téléphonique voient normalement s'afficher le numéro de l'appelant. Cette fonction doit être saluée, puisqu'elle permet à l'appelé de décider avec qui et à quel moment il désire communiquer. La transmission du numéro de l'appelant ne peut cependant pas être imposée, étant donné que dans certains cas la communication de ce numéro risque de révéler des informations sensibles (par ex. chez quel médecin ou avocat l'appelant se trouve lors de l'appel, etc.). L'appelant devrait pouvoir décider à chaque appel s'il accepte que le numéro soit communiqué ou non. Cette possibilité est déjà offerte aux détenteurs de raccordements téléphoniques numériques. Swisscom nous a assuré que les personnes disposant d'un raccordement analogique obtiendront la possibilité de supprimer de cas en cas la communication du numéro de l'appelant dans le courant de cette année (1998). Reste à relever que l'appelé a bien sûr le choix de décider s'il accepte un appel pour lequel l'affichage du numéro de l'appelant a été supprimé. La nouvelle loi sur les télécommunications prévoit même que l'appelé doit avoir la possibilité de refuser de manière générale tous les appels effectués avec une suppression de l'affichage. Nous saluons cette possibilité. Par contre, notre exigence relative à la gratuité de la suppression de l'affichage du numéro de l'appelant n'a toujours pas été remplie. Le DFTCE avait déclaré dans une décision de mars 1997 que la perception d'une taxe unique pour la mise en service était légitime. Un recours contre cette décision a été déposé par des clients de Swisscom auprès de la Commission fédérale de la protection des données (CFPD). Jusqu'à la date limite de rédaction de ce rapport, la commission n'avait pas encore pris de décision.
Il faut également relever ici que Télécom PTT (aujourd'hui Swisscom) a malheureusement omis de rendre attentif aux voies de droit (possibilité de recourir auprès de la CFPD), lorsqu'ils ont satisfait à l'obligation d'informer leur clientèle de la décision prise par le DFTCE.

3.5. Identification/enregistrement des utilisateurs de NATEL easy?

Au moyen d'une disposition rajoutée au dernier moment dans une ordonnance, on a tenté d'enregistrer l'identité de clients de NATEL easy. Cette disposition ne suffit cependant pas pour obliger Swisscom à enregistrer les données des premiers acquéreurs d'une carte à puce NATEL easy et à conserver ces données à l'intention des autorités de justice et de police.

Au début de l'année 1998, une disposition de la nouvelle ordonnance sur les télécommunications qui venait d'entrer en vigueur a créé une certaine confusion. L'article 49 de l'ordonnance stipule: «Les fournisseurs de services de télécommunications doivent identifier leurs abonnés lors de la conclusion du contrat». Cet article a été rajouté peu avant que l'ordonnance soit approuvée. Le projet soumis à la consultation des offices en été 1997 ne contenait aucune exigence de cette sorte. Manifestement, cet article a été demandé par le Ministère public de la Confédération dans le but de pouvoir enregistrer l'identité des clients de NATEL easy ou au moins des premiers acquéreurs de cette carte à puce.
Si l'on examine la manière dont cet article de l'ordonnance a été formulé, on constate qu'il ne saurait être appliqué aux acheteurs de cartes NATEL easy, ces acheteurs n'entrant pas dans une relation de client avec le fournisseur Swisscom. Il suffit d'acheter un appareil de téléphone mobile et une carte à puce (GSM card). Cette carte peut être rechargée de manière anonyme avec le montant désiré. La

carte à puce ne doit pas forcément être achetée auprès de l'exploitant de réseau Swisscom, étant donné que la carte est disponible par d'autres canaux de vente, tels que les commerces spécialisés en électronique. La question se pose en outre de savoir comment le terme «identifier» utilisé dans l'ordonnance doit être interprété. En tous les cas, il n'est pas possible d'en déduire une obligation d'enregistrer et de conserver les données des acheteurs de NATEL easy et de les tenir à la disposition des autorités.
Mis à part cela, un enregistrement des premiers acheteurs serait plutôt inefficace puisque les appareils et les cartes à puce peuvent sans autre être transmis d'une personne à une autre. L'acheteur initial et l'utilisateur ne seront donc pas forcément identiques. Il serait en outre disproportionné d'entreprendre de gros efforts pour créer de nouveaux fichiers, dont l'utilité dans la lutte contre le crime serait faible et qui pourraient mener à suspecter des tiers non coupables.

3.6. Caméras en temps réel sur Internet

Les caméras opérant en direct sur le World Wide Web doivent être installées de manière à ce que les personnes filmées ne puissent pas être reconnues ou qu'elles aient auparavant donné leur accord. Elles doivent avoir été informées que leur image peut être vue dans le monde entier.

On trouve dans le World Wide Web (WWW) un grand nombre de caméras prenant des images sur le vif (LiveCams). Il s'agit de caméras vidéo qui injectent des images sur le réseau soit à intervalles réguliers, soit à la demande d'un utilisateur. Les images pouvant être visionnées par l'intermédiaire de ces caméras en direct sont la plupart du temps prévues pour distraire le public et contribuer à rendre les sites Web plus attrayants.
Une personne nous a contactés pour des caméras en direct installées dans des lieux publics. Elle se sentait atteinte dans sa liberté de mouvement et craignait un usage abusif de ces caméras à des fins de surveillance.
Les images d'une caméra en direct sont accessibles dans le monde entier par le Web et peuvent être traitées de manière incontrôlée par tout utilisateur d'Internet. La qualité des images varie en fonction du système utilisé: certaines caméras sont installées de manière fixe et ne permettent pas à l'usager d'Internet de choisir un angle de prise de vue. D'autres caméras par contre sont orientables par l'utilisateur et/ou permettent de faire un zoom sur un plan.
Nous avons constaté qu'il existe des caméras qui permettent, ne serait-ce que dans certaines conditions (par ex. avec la fonction zoom), de reconnaître des personnes. Souvent les caméras installées ne sont pas visibles des personnes filmées. Elles n'ont donc pas connaissance du fait qu'elles sont prises en image ni à quelle fin, et surtout elles ignorent complètement que leur image peut être captée dans le monde entier par le biais d'Internet. Nous avons constaté qu'une caméra en direct installée dans un grand magasin montrait même des employés dans le champ de vision.
Il est interdit de rendre accessibles sur Internet des données personnelles captées par des caméras en direct sans le consentement des personnes concernées. Ce consentement ne peut en outre pas être obtenu par intimidation. Si la personne concernée doit craindre certains préjudices au cas où elle refuse de se laisser filmer par la caméra, le consentement est considéré comme nul. Une situation très délicate se pose lorsque des employés sont filmés par une caméra en direct dans l'exécution de leur travail. Pour des caméras en direct installées dans des lieux publics, l'obtention d'un consentement semble chose presque impraticable. Dans ces cas, il y

a lieu de garantir par des mesures techniques et organisationnelles que les personnes prises en image ne puissent pas être identifiées.
Le PFPD prévoit donc les possibilités suivantes pour une utilisation conforme à la protection des données de caméras en direct installées dans des lieux ouverts au public (tels que par ex. des rues, places de parc, gares, grandes surfaces, etc.):

1. La caméra en direct doit être installée de manière à ce qu'aucune personne (ni objet qui permettrait d'identifier une personne) ne puisse être identifiée.

2. Au cas où une identification de la personne est possible :
   - cet état de fait doit être apparent pour la personne qui doit être filmée par la caméra ;
   - la volonté de ne pas être filmé doit être respectée en tout temps ;
   - une information claire doit avoir lieu avant que la personne n'entre dans le champ de la caméra ;
   - la personne concernée doit pouvoir décider en toute liberté si elle accepte d'être filmée par la caméra. Cela signifie qu'il n'est pas permis d'installer des caméras en direct qui permettraient une identification des personnes filmées à des endroits de passage obligés.
   - les prises de vue captées ne doivent pas être conservées par l'exploitant de la caméra.

3.7. Postfinance – Conditions générales

A moins que les clients ne le leur aient interdit – après information préalable – la Poste Suisse a le droit de communiquer leur adresse à des tiers. Dans le domaine du trafic des paiements (Postfinance), nous avons constaté que cette information est insuffisante et demande à être améliorée.

Depuis le début de 1998, la Poste Suisse a une nouvelle forme juridique. Dans ses relations avec sa clientèle, elle s'appuie entre autres sur des conditions générales (CG). Fin 1997, les clients du service du trafic des paiements (Postfinance) ont reçu les nouvelles CG par la poste. Au point 17, on peut lire sous l'en-tête «Protection des données»: «Sauf avis contraire, la Poste a le droit de communiquer à des tiers le nom et l'adresse de ses clients». Nombre de détenteurs d'un compte de chèques postal ont été choqués par cette disposition et se sont adressés à nous. Ils n'avaient pas non plus compris comment ils devaient procéder pour obtenir que cette communication de données soit bloquée.
Sur la base d'une ordonnance relative à la loi sur la poste, la Poste a le droit explicite de communiquer à des tiers les adresses postales de clients, à moins que ces derniers n'aient interdit cette communication suite à une information préalable. Par contre l'information dans les CG mentionnées plus haut est insuffisante. Il faut trouver un meilleur moyen de s'assurer que le client prenne connaissance du fait qu'une absence de réaction de sa part autorise la communication de ces données. Nous avons donc proposé à la Poste une solution qui garantit que cette information soit bien reçue. La Poste pourrait par exemple envoyer à sa clientèle une carte-réponse qui pourrait être utilisée pour faire part de sa volonté de ne pas autoriser la communication des données en question. La Poste nous a assuré qu'elle améliorerait l'information dans ce domaine.

4. Personnel

Administration fédérale

4.1. Systèmes de saisie des prestations dans l'administration fédérale

Du point de vue de la protection de la personnalité, les systèmes de saisie des prestations constituent un problème dans la mesure où une saisie détaillée peut permettre de tirer des conclusions sur le comportement d'une personne. Il peut en découler une atteinte disproportionnée à la sphère privée sur le lieu de travail, atteinte non admise par les directives de l'Organisation internationale du travail (cf. annexe, p. 228) et le droit de la protection de la personnalité. En vue de l'introduction de ces systèmes, nous avons érigé des garde-fous destinés à protéger la personnalité.

Divers services de l'administration fédérale introduisent actuellement des systèmes de saisie des prestations. Le but premier de ce genre de systèmes est d'atteindre une meilleure répartition des ressources humaines et financières à partir d'un calcul coûts/prestations. Il ne s'agit donc pas fondamentalement d'un contrôle des collaborateurs, mais d'un «controlling» au sens où l'entend le New Public Management. Cependant, les multiples possibilités de traitement qu'offrent les systèmes permettent justement d'établir aussi des profils détaillés des utilisateurs (entre autres par une saisie systématique des absences, de la formation, des prestations, etc.). Bien qu'il faille effectuer ces évaluations de la manière la plus anonyme possible, les systèmes de saisie des prestations ne sont pas sans danger du point de vue de la protection de la personnalité. Les profils d'utilisateurs ainsi établis peuvent entre autres permettre des déductions sur le comportement des personnes concernées. Mais, tant selon le droit fédéral qu'en vertu des directives de l'Organisation internationale du travail à Genève, le contrôle du comportement est interdit. Les systèmes de saisie des prestations sont conformes avec la protection de la personnalité lorsque les conditions suivantes sont respectées de manière cumulative:

Il faut empêcher le contrôle du comportement de sorte que les supérieurs hiérarchiques ou chefs de section ne puissent pas consulter les données saisies sur leurs collaborateurs.

L'accès à ces données doit si possible être limité à une seule personne (le ou la 'team assistant') de la division en question. La fonction de 'team assistant' consiste essentiellement à contrôler si les données saisies sont complètes, à les réunir et à les transmettre sous forme anonyme à l'organe chargé de leur évaluation. Idéalement, la personne chargée du contrôle de la saisie du temps devrait aussi assumer la fonction de 'team assistant'. Ce dernier doit détruire les données non anonymisées et les copies éventuelles au plus tard un an après leur réunion.

Les différentes rubriques d'absence (vacances, accident, maladie, ...) doivent être regroupées puisqu'un motif détaillé de l'absence est déjà donné avec la saisie du temps. Il convient par ailleurs de ne saisir et d'évaluer que le temps de travail brut.

Il ne faut pas évaluer spécialement les heures improductives (pauses et autres). En effet, dans l'optique d'un controlling, seuls comptent les coûts globaux d'un projet. Ceux-ci englobent aussi les heures improductives, que l'employeur doit dans tous les

cas prendre à sa charge. La saisie des coûts globaux accroît le taux d'acceptation du système de saisie des prestations et diminue le risque de saisies sciemment faussées par les collaborateurs (exactitude des données).

Les données à saisir relatives au volume de travail doivent être déterminées clairement par un service central (postes ou rubriques auxquels elles sont imputées). Il faut définir tout aussi clairement les responsabilités à tous les niveaux ainsi que le but dans lequel les données seront utilisées.

En outre, il convient d'émettre un règlement de traitement et des directives à l'intention des utilisateurs du système.

Par ailleurs, du fait qu'au niveau d'un service ou d'une section on traite des données non anonymisées, les systèmes de saisie des prestations nécessitent une base légale. Nous avons suggéré de créer cette base légale dans le cadre de la révision en cours de la loi sur le statut des fonctionnaires.

Le droit d'être entendu du personnel ou de ses représentants doit être garanti conformément à la circulaire de l'Office fédéral du personnel du 26 mars 1984 (cf. également Rapport d'activités 1993/94, p. 140). La seule information du personnel sur l'introduction d'un système de saisie des prestations ne suffit pas. Le personnel doit aussi avoir la possibilité de s'exprimer sur l'introduction d'un tel système.

4.2. La communication de données concernant les chômeurs sur Internet

L'Office fédéral du développement économique et de l'emploi (OFDE), anciennement OFIAMT, a permis à des bureaux de placement d'accéder sur Internet à des profils de la personnalité des chômeurs qui sont même devenus accessibles au niveau mondial en septembre 1997. Nous avons recommandé à l'OFDE de rétablir la protection d'accès et de renoncer à des traitement de données sensibles sur Internet. Par ailleurs, l'office ne doit pas traiter des données qui n'ont pas de rapport avec le placement de ces personnes.

Fin septembre 1997, nous constations que des données concernant des chômeurs, dont certaines très sensibles, étaient accessibles dans le monde entier sur Internet et sans protection d'accès. Les données provenaient du système d'information sur le marché du travail PLASTA de l'OFDE, dont l'objectif est le placement de la main d'oeuvre. Outre les champs de données licites, on pouvait y trouver des données sensibles qui n'avaient aucun rapport avec le placement de main d'oeuvre. Ainsi des chômeurs y étaient nommément cités (y compris leur numéro AVS) . En outre, le système PLASTA contenait des données sur des poursuites et sanctions pénales (par ex. «a fait environ 3 ans de prison, au pénitencier de Hinwil»), sur la santé («souffre de maux de tête chroniques», «à la clinique psychiatrique de Meiringen» et «mari très dépressif»), mais aussi d'autres informations comme «a trois enfants à charge", „motif de licenciement» ou «à examiner éventuellement pour abus». Nous avons instamment demandé à l'office responsable de ce système de rétablir immédiatement la protection d'accès. Parallèlement, nous lui avons recommandé par écrit de limiter la possibilité de consulter les données PLASTA sur Internet aux services habilités à y accéder et à contrôler régulièrement l'efficacité de la protection d'accès. Nous avons ensuite enjoint à l'OFDE de supprimer entièrement dans Internet la rubrique «Texte supplémentaire libre». Cette recommandation était

motivée essentiellement par le fait que les données PLASTA ne peuvent être rendues accessibles sur Internet qu'à des bureaux de placement privés et uniquement sous forme anonyme. La publication des données en question contredisait du reste les intérêts des chômeurs et constituait aussi dans certains cas (données sur la grossesse, etc.) une infraction à la loi fédérale sur l'égalité entre femmes et hommes (LEg).
Au début du mois d'octobre 1997, nous avons examiné la question de la base légale de la communication de données relatives à des chômeurs sur Internet. Cette communication permet à des bureaux de placement privés d'avoir accès durant un temps illimité à des profils de la personnalité de chômeurs. L'anonymat des profils publiés n'est également pas garanti. D'une part, ainsi que nous l'avons constaté dans notre recommandation du 26 septembre 1997 (cf. p. 112), l'identité des personnes concernées est communiquée dans de nombreux cas. De l'autre, lorsque les profils de la personnalité sont publiés sans identité, il est parfois assez aisé d'identifier les personnes concernées.
Dans ces conditions, nous avons attiré l'attention de l'OFDE sur le fait que les données PLASTA ne doivent pas être accessibles sur Internet sans base légale suffisante. Celle-ci est aussi nécessaire lorsque le consentement des personnes concernées est donné. Néanmoins, si l'OFDE entend maintenir la communication de profils de la personnalité sans base légale, il convient de veiller à ce que les personnes concernées ne soient plus identifiables ou au prix d'efforts démesurés. L'OFDE nous a soumis dans ce sens un nouvel assemblage de données concernant les chômeurs qui peut désormais être qualifié d'anonyme. Enfin, nous avons demandé que la rubrique «Texte supplémentaire libre» soit supprimée entièrement dans l'ordonnance PLASTA.

4.3. Travaux de révision dans la législation sur les fonctionnaires et système BV-PLUS

Dans le cadre de la révision de la loi sur le statut des fonctionnaires, nous nous sommes prononcés sur l'introduction d'un système centralisé de traitement des données (cf. Rapport d'activités 1996/97, p. 148 ss), ainsi que sur le traitement de données relatives à la santé dans l'administration fédérale. Nous avons notamment souligné la nécessité de réglementer clairement les compétences entre l'Office fédéral du personnel et les autres services du personnel de l'administration fédérale. Une décision du Département fédéral des finances est encore attendue. Le traitement des données relatives au personnel de la Confédération ne sera pas réglementé d'ici le milieu de l'année 1998.

L'Office fédéral du personnel nous a soumis au cours de l'année 1997 un projet de nouvelle loi sur le personnel de la Confédération. Nous publions ci-dessous un résumé de nos considérations en matière de protection des données, en particulier quant au système de traitement des données du personnel de l'administration fédérale (système d'information du personnel) ainsi qu'au traitement d'informations relatives à la santé.

Le système d'information du personnel de l'administration fédérale

Le traitement de données personnelles sensibles ou de profils de la personnalité par les organes fédéraux requiert une base légale au sens formel. Cette exigence

accrue de base légale à propos de ce système s'avère également nécessaire du fait que les données traitées peuvent être rendues accessibles en partie par procédure d'appel. Tout d'abord, la base légale doit répartir les compétences entre l'Office fédéral du personnel et les autres services du personnel agissant au niveau des départements et des offices en matière de traitement des données. Ce n'est qu'ensuite qu'on pourra fixer légalement des buts clairs pour les systèmes centralisé et décentralisés de traitement des données dans l'administration fédérale. Par arrêté du 19 décembre 1997, le Conseil fédéral a déclaré obligatoire l'utilisation du logiciel standard SAP R/3 HR pour le soutien informatique du secteur du personnel de l'administration fédérale générale. Selon cet arrêté, il est prévu de mettre en place un système central qui couvre les fonctions communes à tous les domaines et les besoins centraux. Les départements, groupements et offices peuvent utiliser individuellement les autres fonctions du logiciel standard. Nous avions déjà soutenu cette solution dans notre recommandation du 4 juillet 1996 et proposé de ne mettre en place le système central d'information du personnel que pour la gestion des salaires. Au début 1998, nous avons prié le Département fédéral des finances de préciser l'arrêté fédéral dans le sens de notre recommandation. La décision est encore attendue.

La répartition des compétences en relation avec le traitement des données dans l'administration fédérale ne ressort pas du projet de loi sur le personnel de la Confédération. Par conséquent, les buts différents des systèmes centralisé et décentralisés à mettre en place n'apparaissent pas non plus dans le projet de loi.

Nous avons proposé de réglementer comme suit le traitement des données dans l'administration fédérale:

[1]L'Office fédéral du personnel traite en collaboration avec les services du personnel de l'administration fédérale les données personnelles nécessaires à la gestion du personnel de la Confédération. Ces services peuvent traiter des profils de la personnalité ainsi que des données relatives à la santé, à des mesures d'aide sociale et à des mesures de droit administratif, pénal et des poursuites dans la mesure où c'est indispensable à l'accomplissement de leurs tâches légales.

[2]L'Office fédéral du personnel gère un système d'information du personnel (BV-PLUS) destiné au traitement des données requises par la gestion des salaires du personnel fédéral.

[3]Les services du personnel de l'administration fédérale sont chargés du traitement des données dans les autres domaines de la gestion du personnel. A cet effet, ils exploitent leurs propres systèmes d'information du personnel. Si l'occupation d'un poste le requiert, ils peuvent, avec le consentement de la personne concernée, faire établir une analyse graphologique ou procéder à des tests de la personnalité.

[4]Les services du personnel de l'administration fédérale peuvent être raccordés par procédure d'appel au système BV-PLUS pour la gestion des données du personnel fédéral. L'accès d'un service du personnel est limité aux données concernant le personnel pour lequel il est compétent.

[5]Dans la mesure où il n'existe pas de base légale, l'Office fédéral du personnel et les services du personnel de l'administration fédérale ne communiquent des données personnelles à des tiers que si la personne concernée a donné son consentement.

[6]Le Conseil fédéral réglemente les détails, notamment le cadre, les conditions et les services habilités à traiter des données sensibles et des profils de la personnalité conformément aux alinéas 1 et 3. Le Conseil fédéral réglemente en outre la responsabilité de la protection des données, le catalogue des données à saisir et leurs délais de conservation, le droit d'accès, la communication des données, l'organisation et l'exploitation des systèmes automatisés de l'Office fédéral du personnel et des services du personnel de l'administration fédérale, la collaboration avec les autorités participantes et la sécurité des données.

Le traitement des données relatives à la santé dans l'administration fédérale

Le traitement de données relatives à la santé dans l'administration fédérale doit figurer dans la loi sur le personnel de la Confédération du fait de la protection particulière dont ces données bénéficient. La loi doit à ce propos nommément désigner le service fédéral responsable de la protection des données, souligner le caractère confidentiel des données relatives à la santé et réglementer la communication des données à l'intérieur et à l'extérieur de l'administration fédérale. La nouvelle disposition doit être formulée sur le modèle de l'ordonnance sur le Service médical de l'administration générale de la Confédération, sans toutefois faire référence au droit douteux de consultation du chef de service des données relatives à la santé de ses collaborateurs. Nous avons proposé de supprimer ce droit à l'occasion de la prochaine révision de l'ordonnance citée.

En outre, la communication de données à des services extérieurs de l'administration fédérale et aux tribunaux doit en premier lieu être soumise à l'accord écrit de la personne concernée. Le Département fédéral des finances ne peut autoriser le service médical à communiquer des données que de manière subsidiaire, après une pesée des intérêts en jeu. Celle-ci peut avoir lieu lorsque le destinataire des données rend vraisemblable le fait que la personne concernée refuse le consentement ou bloque la communication afin de l'empêcher de faire valoir ses droits ou de sauvegarder d'autres intérêts dignes de protection; il faut donner si possible auparavant l'occasion à la personne concernée de prendre position. Elle doit dans tous les cas être informée de l'autorisation.

Nous avons proposé de soumettre le traitement de données relatives à la santé dans l'administration fédérale à la réglementation suivante:

[1]les données relatives à la santé et les dossiers médicaux du personnel de la Confédération sont conservés auprès du Service médical de l'administration fédérale. Ils sont traités confidentiellement.

[2]Si cela est nécessaire à l'appréciation de l'aptitude à être engagé dans l'administration, à être admis dans la caisse d'assurance ou à exercer les fonctions confiées, ou encore à la décision sur des réclamations découlant des rapports de services, le Service médical de l'administration fédérale peut donner au service intéressé des renseignements sur les conclusions tirées de constatations médicales.

[3]La communication de données relatives à la santé et de dossiers médicaux à d'autres services de l'administration fédérale et à des tribunaux n'est autorisée qu'avec le consentement écrit du candidat ou de l'agent intéressé.

[4]Si la personne concernée ne consent pas à la communication de données, le Service médical de l'administration fédérale peut être autorisé par le Département fédéral des finances à communiquer les données. La communication sera refusée lorsque:

- *l'agent au sujet duquel des renseignements sont demandés a un intérêt prépondérant au maintien du secret,*
- *la communication gênerait dans une mesure importante l'administration dans l'exécution de ses tâches ou*
- *des intérêts publics le requièrent.*

4.4. Publication des primes spéciales et des promotions dans l'administration fédérale

La communication interne à un office de primes spéciales et de promotions par les organes de la Confédération est considérée comme une communication dans un cas d'espèce de données personnelles. Les primes spéciales comme les promotions peuvent être publiées au niveau interne avec l'accord des personnes concernées. Une base légale n'est pas nécessaire si la personne concernée a donné son consentement.

Un office fédéral nous a demandé si la communication interne de l'identité des bénéficiaires de primes spéciales ainsi que des collaborateurs promus était compatible avec la protection des données. Selon la loi fédérale sur la protection des données, les organes fédéraux ne peuvent communiquer des données personnelles que s'il existe une base légale. Exceptionnellement, les organes fédéraux peuvent notamment communiquer des données personnelles sans base légale lorsque la personne concernée y a consenti ou si les circonstances laissent présumer un tel consentement. La publication autorisée par la personne concernée ne doit en outre avoir lieu que de cas en cas. La personne concernée peut toutefois donner son consentement pour plusieurs communications si les circonstances de la communication sont claires et s'il s'agit d'un cas concret. En revanche, un «consentement global» accordé aveuglément ne suffit pas. Etant donné son caractère particulier de rareté, la publication de la prime spéciale doit être considérée comme communication dans un cas d'espèce. Quant à la publication de l'identité du bénéficiaire de la prime, du motif de son octroi ainsi que de son montant, il faut donc que celui-ci donne son consentement. Sans ce consentement, il convient de ne procéder à une publication que s'il existe une base légale au niveau d'une ordonnance.
La publication des promotions est soumise aux mêmes conditions que la publication des primes spéciales. Leur communication a lieu uniquement au sein de l'unité administrative en question et uniquement deux fois par an. Elle est donc clairement délimitée tant dans sa fréquence que dans son extension spatiale. Le consentement de la personne concernée est donc accordé pour un cas concret de communication. Sans ce consentement, la communication des promotions ne peut avoir lieu que s'il existe une base légale.

4.5. La transmission, aux autorités de poursuite, de données relatives aux assurances sociales

Les autorités de poursuite veulent - sur la base d'une nouvelle disposition de la LP – avoir accès aussi à des données relatives aux assurances sociales. Mais dans la mesure où la législation sur les assurances sociales n'autorise pas de communication expresse de données, aucune donnée ne doit être transmise aux autorités de poursuite.

Nous avons rédigés plusieurs avis à ce propos et voudrions en particulier renvoyer le lecteur à notre expertise figurant en annexe au présent rapport (cf. p. 231). Récemment, le Tribunal fédéral a jugé licite la communication, aux autorités de poursuite, de données relatives aux assurances sociales.

4.6. Ouverture du courrier privé par l'employeur

Le courrier privé qu'un employé de la Confédération reçoit à son bureau bénéficie d'une protection illimitée. On doit néanmoins pouvoir reconnaître clairement la nature privée d'un envoi postal. Si sur l'enveloppe, seul le nom précède l'adresse, le caractère privé de l'envoi n'est pas visible.

Le Département fédéral des finances nous a demandé s'il fallait différencier le courrier privé du courrier professionnel et de quelle manière. Nous avons répondu comme suit à cette question: le courrier privé jouit d'une protection illimitée (secret postal). Il doit donc être transmis à son destinataire non ouvert. Si malgré tout, le courrier privé est ouvert par des tiers, il y a atteinte illicite à la personnalité. Celle-ci peut faire l'objet d'une procédure de droit administratif (article 25 LPD) ou de droit pénal (article 179 CP). La lecture au scanner du courrier privé constitue une menace particulière pour la personnalité; en effet, il peut y avoir dans ce cas communication systématique et illicite de données à des tiers. Le courrier privé est un envoi dont on reconnaît qu'il a été adressé à un fonctionnaire non dans sa fonction publique, mais en tant que particulier. Les signes de reconnaissance du courrier privé sont:

- des mentions telles que «privé, personnel, à remettre en mains propres»
- le genre d'envoi (faire-part de décès, journal ou revue adressée nominativement) ou des caractéristiques extérieures (petit format, papier couleur, cartes postales);
- courrier militaire adressé à un agent.

L'intitulé «Monsieur X, Service Y» ne permet donc de conclure à un contenu personnel que si cela est exprimé par un complément («personnel, privé, c/o», etc.). Ecrire en premier lieu le nom du fonctionnaire ne suffit pas à indiquer que le courrier lui est adressé en tant que personne privée (ATF 114 IV 16). Si des doutes subsistent sur le caractère de l'envoi, celui-ci ne sera pas ouvert, mais remis à son destinataire avec une note d'accompagnement. Le destinataire devra immédiatement indiquer sur cette note le caractère de l'envoi et faire enregistrer les documents s'il s'agit de documents de service.

Secteur privé

4.7. Communication illicite de données personnelles durant la procédure de candidature

Le destinataire d'un dossier de candidature ne doit pas communiquer de données personnelles extraites de ce dossier à l'employeur actuel du candidat, surtout lorsque la communication de données est susceptible de faire du tort au travailleur.

Un employé se présente à une nouvelle place. Son dossier de candidature contient, outre les documents usuels, des lettres de clients provenant de son activité professionnelle en cours. Il considère ces lettres comme lettres de référence. Mais du point de vue du devoir de discrétion, ces dernières n'auraient dû être communiquées qu'après avoir été rendues anonymes. Avocate de profession, la destinataire fut priée par le candidat de traiter les documents confidentiellement. Malgré cette requête, elle informa l'employeur du moment du contenu du dossier de candidature. Ce dernier fit pression sur son collaborateur et le poussa à démissionner. Après avoir été avisés de ce cas, nous avons informé l'avocate et employeur potentiel de la manière de traiter des données personnelles dans les rapports de travail:

en vertu des principes de proportionnalité et de finalité, l'employeur ne peut traiter (en particulier communiquer) des données personnelles sur le travailleur que si elles concernent son aptitude à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail. Il ne doit notamment pas s'écarter de ces principes si l'employé s'en trouve défavorisé. La communication de données personnelles extraites du dossier de candidature par l'employeur potentiel, en l'occurrence l'avocate, à l'employeur actuel n'était pas nécessaire à l'exécution du contrat de travail, ni à la procédure de candidature et a occasionné un dommage considérable à la personne concernée. La violation de la protection des données doit être qualifiée d'autant plus grave que la communication a eu lieu contre la volonté expresse de la personne concernée et sans motif justificatif. En outre, une avocate est censée manier des données personnelles avec beaucoup de précaution et une grande réserve. Dans ces circonstances, la personne concernée peut invoquer les prétentions du droit de la personnalité (notamment en vue d'une action en dommages-intérêts). Ces prétentions peuvent être exercées devant le juge civil comme devant les prud'hommes. La procédure devant les prud'hommes est rapide et gratuite.

4.8. Surveillance des employés à la place de travail

La surveillance du personnel par l'employeur doit respecter un certain nombre de règles juridiques. Elle ne doit surtout pas empiéter sans motif justificatif sur la sphère privée de l'employé. On entend notamment par motifs justificatifs le contrôle des prestations ou le contrôle pour des raisons de sécurité. L'employeur a en outre le devoir d'informer au préalable les personnes concernées des mesures de surveillance. Par contre, s'il soupçonne concrètement un comportement contraire à la loi, il peut sans information préalable de la personne concernée procéder à des traitements de données à des fins de conservation de la preuve. Dans ce cas, le traitement ne peut avoir lieu qu'avec la participation ou l'autorisation des autorités pénales compétentes. Cette réglementation s'applique dans le domaine privé comme dans le domaine public.

On nous a demandé à plusieurs reprises de nous prononcer sur l'admissibilité de la surveillance à la place de travail. Nous sommes parvenus aux conclusions suivantes (cf. également Rapport d'activités 1996/97, p. 145 ss): font partie de la sphère privée de l'employé les conversations téléphoniques, l'utilisation du réseau Internet ou l'envoi de courrier électronique (e-mail) non professionnels. Sans limitation ou interdiction expresse des activités privées à la place de travail, l'employé est en droit de supposer qu'elles sont admissibles toute proportion gardée et qu'aucune surveillance ne sera effectuée. Par contre, si les activités privées à la place de travail sont limitées ou interdites, la surveillance ne peut être effectuée que dans les conditions suivantes: tout d'abord, l'ensemble du personnel doit être informé de manière explicite - par des directives internes sur l'utilisation du téléphone, du courrier électronique ou d'Internet à la place de travail - de la limitation ou de l'interdiction des activités non professionnelles à la place de travail. Cette information préalable est nécessaire pour des raisons de transparence. Elle découle du principe de la bonne foi et constitue la condition première de l'exercice du droit d'accès. Par ailleurs, la surveillance de la sphère privée de l'employé à la place de travail ne peut avoir lieu qu'à des fins de contrôle des prestations ou pour des motifs de sécurité. Elle peut uniquement être entreprise à des fins d'exécution du contrat de travail et doit être proportionnel. En revanche, le contrôle du comportement n'est pas autorisé.
S'il possède des indices concrets (par exemple les adresses des pages consultées sur Internet, les adresses e-mail ou les numéros de téléphone composés) de l'exercice abusif d'une activité privée durant les heures de travail, l'employeur doit en informer l'ensemble du personnel du service concerné.
A cette occasion, il attirera l'attention du personnel sur le fait que des enregistrements et des relevés peuvent être faits si les abus se poursuivent et que les personnes concernés peuvent faire l'objet de poursuites disciplinaires.
En revanche, la protection de la sphère privée cédera le pas si l'on soupçonne concrètement un comportement contraire au droit, c'est-à-dire qui ne contrevient pas seulement au contrat de travail (et aux directives y afférentes). Par exemple l'employé est soupçonné de fraude, de diffamation ou d'un autre délit. Les autorités pénales sont alors autorisées sur demande de l'employeur à effectuer des traitements de données à des fins de conservation de la preuve (par ex. enregistrement de conversations téléphoniques, consultation du courrier électronique, etc.) sans en informer au préalable la personne concernée. Ces mesures ne constituent pas des vérifications pour des motifs de sécurité ou à des fins de contrôle des prestations. Elles se justifient par un intérêt prépondérant public ou privé de l'employeur constaté sur la base d'une pesée des intérêts effectuée par les autorités pénales compétentes. Les données personnelles collectées doivent être traitées de manière confidentielle et détruites dès que le but de l'enregistrement est atteint.

4.9. La vente d'entreprises sous l'angle de la protection des données

On ne peut communiquer des données personnelles dans le cadre de la vente d'une entreprise qu'avec le consentement des personnes concernées. Seules peuvent être communiquées les données personnelles nécessaires à l'évaluation de l'entreprise à reprendre. Si pour des raisons particulières, on ne peut informer les personnes concernées et recueillir leur consentement, la communication n'est possible que sous forme anonyme.

Une entreprise privée nous a demandé de nous prononcer sur les aspects de protection des données dans le cas de la vente d'une entreprise. Dans le contrat de travail, l'employeur ne peut traiter des données sur les employés 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. Toute collecte, conservation et transmission de données sur l'employé qui ne présente aucune relation avec le poste de travail se heurte aux principes de finalité et de proportionnalité. La communication de données dans le cadre de la vente d'une entreprise ne présente aucun lien avec le rapport de travail, à la différence par exemple de la collecte de données à l'occasion d'une procédure de candidature. Elle a lieu uniquement pour permettre aux acheteurs potentiels d'évaluer l'objet. La communication de données ne doit donc avoir lieu qu'avec le consentement de la personne concernée. Ce n'est qu'une fois informées que les personnes concernées peuvent éventuellement s'opposer à la communication de données ou faire valoir leur droit d'accès auprès du nouveau maître du fichier. S'il y a eu consentement, la communication de données personnelles ne peut avoir lieu que dans la mesure où elle peut être utile à l'évaluation de l'objet mis en vente. La portée de la communication dépend du déroulement dans le temps de l'affaire et de la position des personnes concernées dans l'entreprise. Au stade initial des négociations précontractuelles, les données ne doivent être communiquées que sous forme anonyme. Les dossiers complets touchant le personnel peuvent être communiqués au plus tôt immédiatement avant la conclusion du contrat. Il convient de juger de cas en cas si, dans la vente d'une entreprise, l'examen relatif aux personnes est nécessaire et dans quelle mesure il convient de tenir compte du déroulement de l'affaire dans le temps ainsi que de la position des personnes concernées (cadres, personnel qualifié et non qualifié) dans l'entreprise mise en vente.

Si la communication de données a lieu sans information ni consentement des personnes concernées parce que la conclusion du contrat s'en trouverait menacée, elle doit uniquement avoir lieu sous forme anonyme. Si le contrat n'est pas conclu, il faut restituer les documents touchant le personnel et détruire les éventuelles copies. Si les données sont communiquées à l'étranger, on tiendra compte de règles supplémentaires. Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait s'en trouver gravement menacée, notamment du fait de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse. Si des données personnelles doivent être communiquées dans des Etats ne disposant pas d'une protection des données équivalente, il faut garantir cette dernière à l'aide d'un contrat. Si en outre, des fichiers sont transmis à l'étranger, il faut l'annoncer au préalable au Préposé fédéral à la protection des données lorsque cette communication n'est pas soumise à une obligation légale ou que les personnes concernées n'en ont pas connaissance.

Parallèlement aux prescriptions légales, il faut soumettre la communication de données personnelles dans le cadre de la vente d'une entreprise à des mesures d'ordre technique et organisationnel. La confidentialité, la disponibilité et l'exactitude des données doivent être garanties. Il faut en particulier empêcher qu'à l'occasion de la communication des données ainsi que du transport des supports de données, les données soient lues, copiées, modifiées ou effacées sans autorisation. Par ailleurs, il faut garantir que seules les personnes autorisées aient accès aux données traitées.

5. Assurances

Assurances sociales

5.1. Feuilles d'informations et clause de consentement

Les feuilles d'information et les clauses de consentement telles que les assurances privées les connaissaient ont été encore perfectionnées. Des efforts ont été notamment entrepris pour offrir aux assurés une meilleure transparence dans le traitement de leurs données. Par exemple, les compagnies d'assurance sont plus nombreuses à demander à l'assuré une procuration écrite avant de prendre des renseignements auprès des médecins, hôpitaux, etc.

Jusqu'ici, les assurances avisaient leurs clients – si tant est qu'elles le faisaient – par une feuille d'information sur le traitement de données. En outre, quelques assurances se sont déclarées prêtes à requérir le consentement des assurés pour chaque circonstance spécifique (demande d'affiliation, devoir d'annonce, accident, prestation, sinistre, etc.). A ce propos, il convient de se reporter à nos précédents rapports d'activités (cf. 3e Rapport d'activités, p. 148 et 4e Rapport d'activités, p. 153).
Dans la pratique, la feuille d'information s'est avérée efficace. Elle permet aux assurés d'avoir connaissance des flux de données, très confus pour le profane, dans le domaine des assurances et attire leur attention notamment sur le droit d'accès dont ils bénéficient.
Les clauses de consentement ne remplissent pas encore les conditions de transparence requises. Du point de vue de la protection des données, les «procurations en blanc», que l'on rencontre encore couramment, sont nulles; en général demandées au stade initial d'un contrat d'assurance, elles ont pour but d'autoriser l'assurance à procéder ultérieurement à tous les traitements de données.
Les clauses de consentement qui se limitent à une seule circonstance spécifique ne fournissent toujours pas suffisamment d'informations à l'assuré sur le traitement des données le concernant. Même si le client donne son accord pour que l'assurance ne procède à des recherches que dans le cadre d'une demande d'affiliation, il n'est pas mis au courant dans les détails de la suite des démarches. En effet, le consentement permet aux assurances de recueillir des renseignements auprès de plusieurs tiers (médecins, hôpitaux, etc.) sans que l'assuré le sache.
En revanche, la «directive sur la protection des données» élaborée par des spécialistes des assurances répond dans une très large mesure au besoin accru de transparence dans le domaine des assurances et informe véritablement les assurés de leurs droits. Elle précise par ailleurs que la compagnie d'assurance doit obtenir la procuration signée de la personne concernée avant toute demande de renseignement auprès de médecins, hôpitaux, etc.
Les dossiers de l'assurance sont transmis au tiers en question uniquement par l'assuré. De même, les renseignements, rapports et expertises demandés sont d'abord communiqués à la personne concernée. Ce n'est que lorsque celle-ci aura connaissance de leur contenu que les documents pourront être communiqués en général uniquement au médecin-conseil de l'assurance.
L'avantage de cette «directive sur la protection des données» est évident: la personne concernée est informée d'emblée du traitement de données effectué par l'assurance. Elle a donc la possibilité de réfuter à temps une expertise inexacte par exemple et d'intervenir lorsque l'échange des documents entre l'assurance et le médecin est trop important (atteinte au principe de la proportionnalité). Elle peut demander conseil à son médecin ou à son représentant légal et défendre ainsi ses droits. L'éventualité d'un traitement de données illicite par l'assurance s'en trouve diminuée d'autant.

Du point de vue de la protection des données, la «directive sur la protection des données» est donc une heureuse initiative et répond aux besoins d'information de l'assuré. Sa conception actuelle peut sembler compliquée, surtout pour les assurances. Nous connaissons toutefois des cas concrets où cette procédure a été menée avec succès et rapidité.
En outre, nous sommes persuadés que l'on peut améliorer la transparence en matière d'assurance essentiellement par des mesures techniques et organisationnelles sans que cela mène obligatoirement à un surcroît de frais et de démarches administratives.

5.2. L'évolution de la protection des données en matière sociale

D'une part, les dépenses dans le domaine social ne cessent de croître. De l'autre, l'Etat a de plus en plus de difficultés à assumer l'augmentation des coûts sociaux. Il en résulte une pression visant le contrôle des coûts, laquelle se répercute à son tour sur les droits de la personnalité des bénéficiaires de prestations sociales.

Depuis quelques années, la diminution des recettes et l'augmentation des dépenses ont été une source de difficultés pour les budgets de la Confédération et des cantons. Or les coûts des assurances sociales et de la prévoyance sociale n'iront pas en diminuant au cours des prochaines années. Des voix s'élèvent légitimement pour que les prestations sociales soient mieux maîtrisées. Comme les exemples suivants le montrent, ce n'est pas sans conséquence pour la protection des données.
Dans le secteur de la santé, la pression des coûts se traduit toujours plus par des atteintes à la protection des données. Une caisse-maladie a tenté par exemple de «rejeter» les assurés qui lui coûtaient cher vers d'autres caisses.
Pour leur part, les autorités de poursuite et les autorités fiscales requièrent un accès plus large aux données des bénéficiaires d'assurances sociales. Pour nous, une transmission de ces données est envisageable – si tant est qu'elle soit nécessaire - uniquement si une loi au sens formel l'autorise.
Les autorités de prévoyance sociale s'adressent souvent à d'autres institutions (caisses-maladie, etc.) sans avoir au préalable recueilli le consentement du bénéficiaire de l'aide sociale ou étudié suffisamment son cas.
Du point de vue politique, diverses démarches ont été tentées en 1997 surtout au niveau communal afin de lutter contre «l'abus social». En ville de Berne, un responsable politique voulait instaurer un numéro vert pour les citoyens qui auraient pu ainsi dénoncer de manière anonyme par exemple leurs voisins pour «abus social». En ville de Zurich, l'introduction de «détectives sociaux» a été refusée de justesse par le conseil municipal.
Du point de vue de la protection des données, l'évolution actuelle dans le domaine social n'est pas positive. Il est incontesté que les autorités doivent rechercher les moyens de maîtriser les coûts dans le domaine social et de lutter contre «l'abus social». Mais ces moyens doivent être appropriés et nécessaires. Les deux exemples de Berne et de Zurich impliqueraient une grave atteinte aux droits de la personnalité des citoyens concernés. Pour faire obstacle à «l'abus social», il faudrait tout d'abord étudier des mesures qui empiètent moins sur les droits de la personnalité (plus de travail social, analyse plus approfondie des cas, feuilles d'information, etc.). Par ailleurs, il faudrait examiner auparavant ce que l'on entend pas «abus social» et déterminer son ampleur effective.

5.3. La surveillance de l'Office fédéral des assurances sociales en matière de protection des données

Nous avons dans le passé constaté à plusieurs reprises que des doutes régnaient quant à la surveillance du PFPD sur des organes de la Confédération et sur leurs relations avec la fonction d'autorité de surveillance. Nous allons expliquer ci-dessous quelle est à notre avis la seule interprétation possible des prescriptions en vigueur. En résumé, les deux autorités de surveillance doivent être complémentaires parce qu'elles revêtent des fonctions différentes.

Nous allons illustrer le problème par un exemple: les assureurs-maladie selon la LAMal sont des organes de la Confédération non seulement en vertu de la LPD, mais aussi de la LAMal. Il s'ensuit – du moins à première vue – le problème suivant: les assureurs sont soumis d'une part à la surveillance de l'OFAS et de l'autre à la surveillance du PFPD.
Interprétées de manière «spontanée», les prescriptions en vigueur impliqueraient que l'on procède à une séparation selon le domaine de surveillance: le PFPD surveillerait le respect des prescriptions de protection des données et l'OFAS le respect de toutes les autres prescriptions. Cette interprétation ne résiste pas à un examen plus poussé pour plusieurs raisons. Selon le libellé de la norme de surveillance déterminante pour le Conseil fédéral et l'OFAS (article 21, 2e alinéa LAMal), cette surveillance a pour objet l'application uniforme de la loi. Les prescriptions de protection des données comme l'obligation de garder le secret selon l'article 83 LAMal ne sont justement pas exclues. En outre, il faut relever que les prescriptions de protection des données sont disséminées dans les lois les plus diverses dont l'exécution n'est suffisamment connue que d'un office spécialisé comme l'OFAS. Par ailleurs, la LPD contient des principes comme celui de la proportionnalité ou de la bonne foi qui sont applicables à l'ensemble de l'activité administrative. Le respect de ces principes ne peut pas être considéré de manière isolée car les principes sont toujours en relation avec l'exécution de certaines autres réglementations.
Mais surtout, la surveillance de l'OFAS est différente de celle du PFPD. Cela apparaît notamment dans le droit de pouvoir émettre des instructions que les deux genres de surveillance impliquent. La surveillance au sens traditionnel veut que l'organe de surveillance puisse établir des directives à l'égard des différents organes d'exécution. En revanche, le PFPD ne peut qu'émettre des recommandations qui ne sont même pas directement obligatoires. La différence est encore plus nette si l'on considère la compétence d'établir des directives générales. Le PFPD ne dispose pas de cette compétence, alors que l'OFAS peut émettre des directives sous forme de circulaire non pas seulement à l'intention de certains organes d'exécution, mais à l'intention de tous. Cette possibilité doit aussi demeurer pour les questions de protection des données. En effet, il ne peut être dans l'esprit de la LPD – qui a introduit la surveillance exercée par le PFPD – d'exclure en matière de protection des données toute réglementation générale au niveau de la circulaire. D'ailleurs, de telles circulaires existent depuis des années dans des domaines importants du point de vue de la protection des données et de nouvelles circulaires sont émises aujourd'hui encore. L'OFAS conserve donc la surveillance générale sur les organes d'exécution. Parallèlement, le PFPD exerce sa surveillance en complément et assiste aussi à titre consultatif l'OFAS, à l'instar d'autres offices, en matière de

protection des données. Nous avons à plusieurs reprises informé l'OFAS de nos conclusions.
Mentionnons pour terminer que l'Office fédéral des assurances privées a également reconnu sa compétence de surveillance globale à l'encontre des assurances privées en matière de protection des données.

5.4. Le «registre-miroir» de l'AVS

La constitution d'un «registre-miroir» de l'AVS devraient permettre de traiter plus rapidement les demandes que les citoyens déposent auprès des caisses de compensation. Si les principes de la protection des données sont respectés, il n'y a rien à objecter à l'introduction du «registre-miroir».

Les caisses de compensation AVS reçoivent de plus en plus de demandes émanant de citoyens. Pour diverses raisons (splitting, etc.), ces derniers veulent des renseignements sur les cotisations AVS qu'ils ont déjà versées. Les contributions des assurés figurent sur des comptes individuels. Ces comptes rassemblent entre autres les données suivantes: nom, no d'AVS, état du compte, durée de contribution, employeur.
Pour certaines caisses de compensation, le traitement de ces demandes est long et difficile. La Confédération a donc lancé le projet de «registre-miroir» de l'AVS grâce auquel toutes les caisses pourront consulter les comptes sur écran. Le «registre-miroir» aurait pour seul but de permettre aux caisses de compensation d'accéder plus rapidement aux comptes. En conséquence, les assurés seraient plus rapidement informés de leurs cotisations.
Nous n'avons fondamentalement rien à objecter au «registre-miroir» de l'AVS dans la mesure où le système informatique requis répond aux exigences posées par la LPD. A cet égard, la sécurité des données doit faire l'objet d'une attention particulière, surtout les contrôles d'accès. Par ailleurs, nous sommes d'avis qu'une modification de l'ordonnance à elle seule ne suffit pas pour mettre en place ce «registre-miroir». En effet, des profils de la personnalité seront alors traités auxquels les caisses de compensation pourront accéder par procédure d'appel. Nous avons donc demandé que soit créée dans la loi sur l'AVS une base légale destinée à ce «registre-miroir».

5.5. La communication de données personnelles par la CNA

Nous constatons de plus en plus souvent dans le cadre de nos activités que la CNA contrevient aux dispositions de la LPD. En particulier, trop de données sont communiquées à des tiers non habilités.

La marge de manœuvre de la CNA dans la communication de données d'assurés à des tiers est surtout une question de proportionnalité. Selon ce principe, on ne doit communiquer que les données personnelles qui sont absolument nécessaires et aptes à atteindre le but déterminé.
Manifestement, ce principe n'est pas respecté lorsque la CNA rend des décisions. Les décisions (y compris les motifs) sur une pension et une indemnité pour atteinte à l'intégrité par exemple ne sont pas remises seulement à l'assuré, mais aussi à l'employeur. De cette manière, des données relatives à la santé sont communiquées – sans justification – à l'employeur. Nous pouvons citer un cas où un employeur a

abusé de cette mise au courant et s'est exprimé avec mépris sur l'assuré en présence des autres collaborateurs.
De même, les formulaires d'accidents de la CNA et d'autres assurances-accidents sont incompatibles avec la LPD. En cas d'accident non professionnel par exemple, l'employeur n'est concerné ni par la cause de l'accident, ni par le genre de blessure (cf. «Formulaire annonce accident LAA»). Pour leur part, les formulaires-accidents de la CNA destinés aux chômeurs ne sont absolument pas conformes à la protection des données. Par exemple, l'indication du chômage de l'assuré sur une feuille de pharmacie est inutile. Le pharmacien n'a pas besoin de savoir que l'assuré est chômeur. Dans les régions rurales surtout, le chômage est encore associé à la perte du prestige social et tout le monde connaît tout le monde. Il s'impose donc de faire preuve de la plus grande réserve dans la diffusion de données sur les chômeurs.
Par ailleurs, il nous est apparu que les assurances responsabilité civile reçoivent trop de données de la CNA en cas de subrogation.
A notre avis, le flux des données dans le domaine de l'assurance-accidents doit être analysé de manière détaillée et examiné du point de vue de sa conformité avec la protection des données. Il convient en particulier de considérer si et dans quelle mesure un échange intensif de données entre la CNA et le destinataire des données est toujours justifié.

5.6. Le droit d'accès en matière d'assurance-accidents

Selon un arrêt rendu par le Tribunal fédéral, les assurances-accidents doivent aussi donner par écrit à leurs assurés les renseignements demandés sous forme d'imprimé ou de photocopie.

Une compagnie d'assurance-accidents refusa de remettre à une assurée son dossier d'accident que ce soit sous forme originale ou photocopiée. En revanche, elle lui donna la possibilité de consulter son dossier sur place.
L'assurée présenta un recours auprès de la Commission fédérale de la protection des données. La commission ordonna à l'assurance de remettre à l'assurée son dossier sous forme écrite. L'assurance-accidents porta le cas devant le Tribunal fédéral, lequel confirma la décision de la Commission fédérale de la protection des données.
Selon le Tribunal fédéral, la récente loi sur la protection des données est ici applicable et non la réglementation jusque-là en vigueur de l'ordonnance sur l'assurance-accidents. Cette ordonnance prévoit que les assurés ne peuvent consulter leurs dossiers qu'au siège de la compagnie d'assurance. En revanche, la loi sur la protection des données, plus récente, requiert que les assurés reçoivent les renseignements demandés par écrit, sous forme d'imprimé ou de photocopie.

5.7. L'organisation interne des compagnies privées d'assurance-accidents

Les assurances privées en Suisse peuvent aussi participer à l'application de la loi fédérale sur l'assurance-accidents obligatoire (LAA). Leurs collaborateurs sont soumis au devoir légal de discrétion même à l'intérieur de la compagnie. L'organisation interne doit donc être conçue de sorte qu'au moins le domaine de l'assurance-accidents obligatoire soit distinct des autres secteurs du point de vue de l'administration et du personnel. Dans le cas contraire, on risque de porter atteinte non seulement au devoir de discrétion, mais aussi aux dispositions de la loi sur la protection des données.

Dans le cadre d'un recours hiérarchique adressé à l'Office fédéral des assurances sociales (OFAS), il fut demandé à une compagnie privée d'assurance-accidents de séparer - du point de vue de l'organisation - l'assurance-accidents obligatoire des autres secteurs d'assurance. Cette requête était surtout motivée par le fait que certains collaborateurs de la compagnie avaient accès à la fois aux dossiers LAA et aux dossiers d'assurance privée des mêmes personnes. Cet état de fait fut considéré comme une violation du devoir de discrétion. En outre, le mode de gestion dans les dossiers mêmes ainsi que l'échange des documents entre les différents dossiers furent jugés obscurs pour les assurés (atteinte au principe de la transparence). L'assurance allégua qu'il était dans l'intérêt de l'assuré que le même collaborateur traite à la fois les dossiers LAA et les autres dossiers. A ses yeux, un collaborateur connaissant tous les dossiers était mieux informé. Donc, dans les faits, il n'y avait pas de séparation, au moins au niveau du personnel, entre le domaine de l'assurance-accidents obligatoire et les autres branches d'assurance.
L'OFAS nous a priés de nous prononcer sur ce cas. A notre avis, les collaborateurs d'une compagnie d'assurance-accidents privée sont soumis au devoir de discrétion également à l'intérieur de l'entreprise. Nous estimons que les assurances-accidents privées doivent respecter les mêmes règles que la CNA par exemple. Au sein d'une compagnie, les collaborateurs dont le domaine n'est pas l'assurance-accidents obligatoire ne doivent donc pas avoir accès aux dossiers LAA, ni recevoir des informations émanant du secteur de l'assurance-accidents. Transmettre des données d'un dossier LAA à un dossier assurance-responsabilité civile - même à l'intérieur de la même compagnie – est incompatible avec le devoir légal de discrétion. Nous estimons qu'il y a déjà violation du devoir de discrétion lorsqu'un même collaborateur fait passer des documents d'un dossier LAA dans un autre dossier. En effet, il y a alors communication, sans motif justificatif, d'informations provenant d'un domaine protégé par la loi.
Par contre, la transmission (ainsi que la collecte) de données provenant d'un dossier d'assurance privée dans d'autres dossiers n'est possible qu'avec le consentement spécifique de l'assuré. Ce dernier doit néanmoins être conscient de la portée de son consentement.
Du point de vue de la protection des données, le manque de transparence du traitement des données constitue le problème majeur. En effet, il est difficile pour le profane de comprendre quel collaborateur traite quel dossier et à quels dossiers il a accès. Il est également difficile de savoir si et dans quelle mesure les dossiers sont échangés à l'intérieur de la compagnie d'assurance. Pour cette raison, nous demandons également que la gestion des dossiers en question soit plus transparente. Les documents doivent être gérés de sorte que la personne concernée - en consultant les documents - puissent avoir une idée concrète de la manière dont les documents circulent (qui a transmis quelles données à qui et dans quel but, ou qui s'est procuré quelles données auprès de qui).

La forme actuelle d'organisation, à savoir la gestion commune des différents dossiers d'assurance, est de nature à contrevenir aux dispositions légales. Au moins le secteur LAA doit être séparé des autres domaines d'assurance du point de vue de l'organisation, du personnel et de l'administration. Nous avons prié l'OFAS en tant qu'autorité de surveillance en matière d'assurance-accidents ainsi que l'Office fédéral des assurances privées (OFAP) en tant qu'instance de surveillance en matière d'assurance privée de coordonner la surveillance et de prendre les mesures nécessaires.

5.8. Documents internes – Documents externes

Dans le domaine des assurances sociales, les procédés régissant l'accès aux dossiers distinguent les documents internes des documents externes. Les documents externes ont le caractère de preuve et sont montrés sur demande à la personne concernée. En revanche, l'assuré ne peut consulter les documents internes qui ont pour but de permettre la formation d'une opinion au niveau administratif interne. Le refus général d'autoriser la consultation des documents internes contrevient néanmoins à la loi sur la protection des données.

Presque toutes les assurances sociales distinguent, à l'intérieur des dossiers des assurés, entre documents internes et documents externes. Cette distinction repose sur diverses circulaires. Les documents externes ont le caractère de preuve pour le traitement du cas (rapports, expertises de diagnostics, constats, etc.). Les documents internes sont uniquement destinés à l'usage interne (travaux préparatoires, demandes, notes, pièces justificatives auxiliaires, etc.). Jusqu'ici, les autorités compétentes en matière d'assurances sociales comme la CNA n'ont permis que la consultation des documents externes.
Selon la loi sur la protection des données, toute personne peut demander à un maître de fichier si des données la concernant sont traitées. Les restrictions du droit d'accès sont réglementées de manière exhaustive. En particulier, l'accès peut être refusé lorsqu'une loi formelle le prévoit. Néanmoins, les diverses lois sur les assurances sociales ne comportent aucune disposition qui autoriserait une limitation du droit d'accès. Cette distinction entre documents internes et documents externes ainsi que le refus général de consultation des dossiers portent donc atteinte au droit d'accès selon la LPD.
Le caractère ouvert et non limitatif des documents externes invite justement l'administration à établir des documents internes. On peut comparer ces dossiers internes avec ce que l'on nomme «textes libres» ou «remarques», dont le volume et le but ne sont pas clairement définis. Les jugements de valeur subjectifs figurant dans ce genre de papiers sont très équivoques. Souvent, ces documents ont une influence déterminante sur la décision à prendre et devraient donc être communiqués à la personne concernée. Par exemple des données fournies par un dénonciateur privé figurant dans un dossier d'assurance-accidents et désignant l'assuré comme un simulateur furent mentionnées sur un papier interne. C'est d'autant plus grave lorsque le droit d'accès est refusé à la personne concernée et qu'elle ne peut se défendre contre ce genre d'affirmation. Dans la mesure où les documents dits internes contiennent des données qui sont utilisées d'une quelconque manière comme base de décision, ils ne doivent pas être définis comme documents internes. Par conséquent, le droit d'accès peut aussi être accordé pour ces documents.

Dans l'optique d'une administration transparente et proche du citoyen, nous nous prononçons pour un droit d'accès complet en matière d'assurances sociales. Nous avons prié l'Office fédéral des assurances sociales en qualité d'autorité de surveillance de prendre les mesures nécessaires et notamment d'adapter en conséquence les diverses circulaires.

5.9 La nécessité des médecins-conseils dans le domaine de l'assurance-maladie

Selon la conception de la loi, les médecins-conseils revêtent deux fonctions importantes dans le domaine de l'assurance-maladie. D'abord ils sont indispensables à la garantie de qualité parce qu'eux seuls sont souvent en mesure de juger si un traitement précis est indiqué. Ensuite – et c'est ici le point important – les médecins-conseils ont la tâche fondamentale du point de vue de la protection des données de servir de filtre lorsqu'il s'agit d'informations véritablement délicates. Pour pouvoir remplir cette fonction, il ne faut pas seulement qu'ils bénéficient d'une position indépendante, il faut aussi garantir que les envois qui leur sont adressés soient ouverts dans le cadre de leur domaine de responsabilité.

Le 16 avril 1997, lors du congrès annuel de la Société suisse des médecins-conseils et à la demande de ceux-ci, le Préposé fédéral à la protection des données s'est exprimé sur la fonction des médecins-conseils dans l'optique de la protection des données. Nous présentons ci-dessous quelques-uns des éléments principaux de son intervention. Conformément à l'article 42, 5e alinéa de la loi fédérale sur l'assurance-maladie (LAMal), le médecin traitant peut dans certains cas fournir des indications d'ordre médical aux médecins-conseils et non à l'administration de la caisse. Dans tous les cas, le fournisseur de prestations doit se conformer à la demande de l'assuré. Néanmoins, l'article 57 constitue une disposition centrale de la LAMal, notamment l'alinéa 5 qui garantit l'indépendance du médecin-conseil, ainsi que l'alinéa 7 qui le charge expressément du respect des droits de la personnalité des assurés. En plus de cette formulation générale, le même alinéa décrit la fonction de filtre des médecins-conseils: ils «ne transmettent aux organes compétents des assureurs que les indications dont ceux-ci ont besoin pour décider de la prise en charge d'une prestation, pour fixer la rémunération ou motiver une décision».
A ce propos, le point important dans la pratique est la fréquence avec laquelle il est fait appel au médecin-conseil. Si celui-ci est trop souvent mis à contribution, il ne sera guère en mesure de remplir son rôle de filtre à propos des informations vraiment délicates. Il sera surchargé d'informations dont au moins une partie ne sont pas à considérer comme sensibles. Dans la situation actuelle, il ne pourrait plus garantir la discrétion, ni filtrer l'information. Donc, pour le moment, les fournisseurs de prestations n'ont qu'une seule solution: adresser les informations délicates au médecin-conseil. Il convient avant tout de requérir de la part de l'assureur qu'il accorde effectivement une position indépendante au médecin-conseil. Ensuite, il doit garantir du point de vue organisationnel que les envois adressés aux médecins-conseils ne soient effectivement ouverts que dans leur sphère de compétence et éventuellement classés par degré de sensibilité. Ces deux mesures ne supposent pas seulement que l'on dégage les fonds nécessaires, mais aussi que les médecins-conseils bénéficient d'une certaine position dans l'organigramme de l'assurance. C'est la seule manière de répondre aux exigences légales mentionnées et de les communiquer aux autres collaborateurs de l'assureur.
A notre avis, il est temps que des services médicaux soient aussi créés dans les autres branches d'assurance. Nous pensons en particulier qu'il est nécessaire que

l'institution du médecin-conseil soit enfin introduite dans l'assurance-accidents obligatoire. Le besoin d'un filtre de sécurité adapté au flux des informations médicales se pose essentiellement pour la CNA, qui constitue la plus importante assurance-accidents de Suisse.

5.10. Les formulaires de proposition d'assurances et le principe de la proportionnalité

Dans leurs formulaires, les compagnies privées d'assurance ne doivent poser que les questions indispensables au contrat. Le principe de la proportionnalité ancré dans la LPD est également applicable aux assurances privées.

Selon la loi fédérale sur le contrat d'assurance, toutes les questions figurant sur le formulaire de proposition sont supposées importantes. Pour la personne qui remplit ce formulaire, il est en pratique très difficile de réfuter cette présomption. Elle répondra donc à toutes les questions (donc aussi aux questions inutiles) afin de souscrire un contrat le plus rapidement possible.
La loi fédérale sur la protection des données a également introduit le principe de la proportionnalité pour le droit privé. Les assurances privées ne doivent par conséquent traiter que les données personnelles appropriées et nécessaire à atteindre le but visé. Les assurances doivent donc s'efforcer de concevoir les formulaires de proposition de sorte qu'ils ne contiennent que les questions vraiment nécessaires.
Malheureusement, nous constatons régulièrement que les professionnels des assurances ne se conforment pas au principe de la proportionnalité. Du fait de la déréglementation touchant certains marchés, les compagnies collectent même des données supplémentaires afin d'adapter au mieux les produits au marché. C'est pourquoi nous avons l'intention d'examiner les formulaires de proposition dans différents secteurs d'assurance du point de vue de leur conformité à la protection des données. Nous prendrons ensuite les mesures nécessaires.

6. Santé

6.1. Commission d'experts pour le secret professionnel dans la recherche médicale:

- Le registre des tumeurs du canton du Valais

Le registre des tumeurs du canton du Valais est en possession d'une autorisation de la Commission d'experts pour le secret professionnel en matière de recherche médicale et est donc autorisé à recueillir des données sur des patients de la région sur lesquels on a diagnostiqué des tumeurs. Une modification prévue de l'infrastructure informatique a été soumise au Secrétariat de la commission d'experts, qui a fait suivre la demande au PFPD pour en examiner la conformité avec la protection des données.

Le système des autorisations de Registres selon l'article 321bis CP n'est déjà pas une affaire simple sur le plan juridique. Expliquée de manière sommaire, une telle autorisation donne au Registre le droit de recueillir auprès des médecins traitants

des déclarations concernant des patients chez lesquels on a diagnostiqué une tumeur. En même temps, cette autorisation permet de lever le secret professionnel des médecins traitants. D'autre part, il est évident pour les neuf autorisations en faveur des Registres des tumeurs que compte la Suisse qu'elles ont également leurs limites. Ainsi, ceux-ci n'ont le droit de traiter leurs données qu'à des fins précises et doivent en particulier garantir que les accès aux données d'identification des patients sont réduits à un minimum et limités à un cercle de personnes très restreint. Nous ne mentionnerons qu'à titre accessoire que le fait qu'une autorisation impose explicitement une telle charge ou que la décision parte implicitement du principe qu'une telle charge va de soi et ne doit pas être formulée comme telle est dû au hasard. Ce régime ne poserait pas de problème s'il ne fondait pas la réglementation des compétences. Car, tant que des charges explicites ont été formulées, il est de la compétence du PFPD d'en surveiller l'application. Dans le domaine des autres limitations par contre, les Registres des tumeurs en tant qu'institutions cantonales sont sous la surveillance des autorités de protection des données des cantons concernés.
Dans son autorisation du 16 août 1995, la commission d'experts se basa sur une structure informatique précise du Registre des tumeurs du canton du Valais. C'est la raison pour laquelle le Secrétariat de la commission fut informé par le registre d'une modification prévue de cette infrastructure. Cette commission à son tour a transmis la demande au PFPD en lui demandant si la modification envisagée était conforme aux exigences de la protection des données.
L'élément principal est la connexion prévue au réseau de l'hôpital cantonal de Sion. Cette question fondamentale trouve en principe déjà réponse lorsqu'on lit attentivement la décision initiale d'autorisation. Il en ressort que la commission avait à l'époque déjà admis qu'une telle connexion aurait lieu tôt ou tard. On peut dès lors arguer que cette connexion se situe tout à fait dans l'esprit de la décision. Ce qui pose problème par contre est la manière imprécise dont la décision a été formulée, selon laquelle «on donne la possibilité au Registre de prendre des données de la Division de pathologie». Ce texte dit très peu sur la fréquence de ces accès (consultations individuelles ou par listes entières) et absolument rien sur les catégories de données concernées. Il n'appartient pas au PFPD de modifier directement les décisions de la commission, raison pour laquelle nous n'avons pas pu préciser cette formulation. Notre réponse dans ce contexte a donc été qu'il fallait garantir au moyen de mesures techniques et organisationnelles que les autorisations d'accès qui avaient été définies ne seraient pas modifiées par la connexion au réseau. Il est bien entendu que ces mesures doivent s'appliquer à l'ensemble du traitement des données et doivent donc en particulier être mises en œuvre et testées aux trois niveaux que sont le réseau, le système d'exploitation et le système de banque de données.

6.2. Ordonnance sur la déclaration des maladies transmissibles de l'homme: défaut de bases légales dans la loi sur les épidémies

Sur la base de dispositions contenues dans l'ordonnance sur la déclaration, l'Office fédéral de la santé recueille des déclarations de maladies contagieuses de la part de médecins et de laboratoires. Dans la mesure où il ne s'agit pas de données anonymisées, ceci nécessite une base légale sous la forme d'une loi au sens formel. Il serait pourtant bon d'examiner au préalable pour toutes les catégories de communications s'il n'est pas possible d'utiliser des données anonymisées.

Dans le cadre de la révision de l'ordonnance sur la déclaration, le PFPD a été consulté par l'Office fédéral de la santé qui en l'occurrence agissait comme organe responsable. Pour nombre de traitements prévus dans l'ordonnance, cette dernière ne constitue pas une base légale suffisante. Dans la mesure où les traitements concernent des données sensibles, ceci nécessite une base légale sous forme de loi. La création d'une telle loi est désormais en vue. La tâche principale du PFPD ne devrait cependant pas consister à devoir insister sur la nécessité de disposer de bases légales à certains niveaux. En créant les bases légales, on gagne bien un peu en transparence; la cause de la protection des données serait cependant mieux servie si certains traitements de données ne nécessitaient d'emblée pas la saisie de données personnelles. En premier lieu, il faut œuvrer afin que les organes traitant les données adoptent un «réflexe de protection des données» qui les amène, lors de chaque traitement, à se poser immédiatement la question de savoir s'il n'est pas possible de travailler avec des données anonymisées. En collaboration avec l'Office fédéral de la santé nous avons, dans le cadre de la révision de l'ordonnance sur la déclaration, pu dégager les cas dans lesquels il n'est pas possible de travailler avec des données anonymisées. Comme on pouvait s'y attendre, il s'avéra également dans ce cas que l'information centrale du point de vue de la protection des données se trouve dans la description des buts poursuivis par un traitement de données. Les tâches de l'Office fédéral de la santé en relation avec la procédure de communication discutée ici peuvent être divisées en deux catégories. D'un côté, il s'agit de poursuivre des objectifs de statistique épidémiologique en observant la propagation de maladies contagieuses. Ces objectifs peuvent en règle générale sans autre être atteints en traitant des données anonymisées, raison pour laquelle la collecte de données personnelles devrait être qualifiée dans ce cas de disproportionnée. D'autre part, il existe certaines maladies qui nécessitent des interventions au niveau des personnes atteintes au cas où ces maladies devaient se déclarer. Dans le cadre de ces déclarations, une communication nominative jusqu'à l'office est nécessaire pour la tâche de coordination de ce dernier et est donc également proportionnée.

6.3. Les statistiques hospitalières H+ sont enfin établies avec des données rendues anonymes

Depuis des décennies, les établissements hospitaliers communiquent à H+ (anciennement VESKA) des données nominatives concernant des patients pour que celle-ci effectue un traitement pour leur compte. Ces communications constituent par principe des actes pouvant être poursuivis pénalement, ce que les intéressés savent depuis longtemps déjà. Cette situation intenable du point de vue juridique a enfin été corrigée après que certaines réflexions concernant la saisie des données pour les statistiques médicales des hôpitaux ont été appliquées de manière analogue pour les traitements effectués auprès de H+.

Depuis 1968, H+ (anciennement VESKA) procède également à des traitements de données de patients pour le compte d'hôpitaux. Ces traitements s'expliquent historiquement par le fait que jusqu'à récemment beaucoup d'établissements hospitaliers ne disposaient pas des ressources informatiques et des connaissances nécessaires pour effectuer eux-mêmes de tels traitements. Que de tels traitements constituaient régulièrement des actes punissables – notamment par la violation du secret professionnel de la part des médecins traitants et de leur personnel auxiliaire – était un fait également connu depuis longtemps. En février 1984 déjà, un groupe

d'experts mandaté par l'Office fédéral de la justice avait publié un rapport intitulé «Protection des données dans le domaine médical», rapport qui soulève deux aspects importants. Il retient que l'élément de fait de la violation du secret professionnel pouvait être considéré comme accompli (p. 166) et que les responsables de la VESKA étaient à l'époque déjà conscients des problèmes (p. 167). Malgré cela, rien n'a été entrepris pendant des années. Le 1er janvier 1998, H+ a enfin introduit une amélioration décisive en appliquant pour ses traitements les mêmes critères d'anonymisation que ceux utilisés pour les statistiques hospitalières. Cela signifie dans un premier temps que les établissements hospitaliers ne peuvent plus faire effectuer des traitements de données nominatives de patients auprès de H+. Ensuite, on renonce également à des données permettant une identification indirecte, telles que la date de naissance exacte ou le numéro postal d'acheminement du domicile. Les numéros de dossier médical tels qu'on les connaît aujourd'hui dans divers hôpitaux sont encore utilisés pendant la durée limitée absolument nécessaire à la validation des données et au contrôle de qualité. Cette démarche devrait nous avoir enfin débarrassés d'un vieux problème très gênant du point de vue de la protection des données, un aspect positif que nous tenons à souligner ici.

6.4. Rapport annuel 1996 de la CNA: mise au point concernant de prétendues déclarations des préposés à la protection des données

Le rapport annuel 1996 de la CNA prenait position sur des déclarations faites par les préposés à la protection des données des cantons et de la Confédération qui en réalité n'avaient jamais été prononcées. La partie concernée du texte du rapport est citée et rectifiée ci-dessous.

Le rapport annuel 1996 de la CNA mentionne à la fin du paragraphe concernant MediData SA que «les exigences de la protection des données ont été entièrement satisfaites». Il va même jusqu'à déclarer que tant le Préposé fédéral à la protection des données que les préposés cantonaux avaient étudié le concept et l'avaient accepté sur le fond. Il faut corriger ici que le PFPD n'a pas fait de déclaration approuvant le concept de la société mentionnée. Le PFPD ne connaît en outre aucun préposé cantonal susceptible d'avoir fait une telle déclaration. Nous savons même de quelques préposés avec certitude qu'ils n'ont pas fait une telle déclaration. La seule prise de position de notre part dans cette affaire a été une contribution dans notre troisième rapport d'activités 1995/96 (p. 157), dans lequel nous mentionnions les aspects suivants. D'une part, nous avons jugé positifs les efforts entrepris pour assurer la sécurité des communications. D'autre part, nous avons émis des réserves concernant des bases légales qui font défaut, le fait que les personnes concernées n'étaient pas intégrées dans le circuit d'information, le volume des données communiquées régulièrement aux assureurs ainsi que la possibilité pour le médecin-conseil, d'assumer sa tâche au service de la protection de la personnalité dans un tel système.

7. Crédits

7.1. Exigences auxquelles doivent répondre les conditions générales et les demandes de cartes de crédit

Les conditions générales et les formulaires de demande de cartes de crédit doivent indiquer clairement à quel genre de traitement seront soumises les données collectées afin que la personne qui dépose la demande de carte sache comment se dérouleront le traitement et la transmission de données la concernant.

On ne peut traiter les données que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. Lorsque les transactions opérées avec une carte de crédit permettent de saisir et d'exploiter des habitudes de consommation ou de voyage dans une optique de marketing sans que le consentement du client ait été auparavant obtenu, il y a modification illicite du but.
Ainsi que nous l'avons constaté, la plupart des détenteurs de cartes de crédit ne savent pas comment se déroule effectivement le traitement de leurs données personnelles et à quels traitements de données ils consentent. En effet, la plupart des demandes de carte et des conditions générales n'indiquent pas clairement l'ampleur du traitement prévu et les destinataires des données. Nous avons attiré l'attention des grandes entreprises de cartes de crédit sur les principes généraux de traitement des données personnelles, sur les motifs justificatifs et les exigences requises par la clause de consentement. Nous avons tout particulièrement souligné le fait que l'utilisation d'une carte de crédit et les traitements de données qui y sont liés génèrent des profils de la personnalité qui permettent d'apprécier des aspects essentiels de la personnalité.
La possession d'une carte de crédit est indispensable pour pouvoir entrer dans certains pays, ce qui restreint de fait le client dans sa liberté contractuelle, en particulier en matière de conclusion du contrat. La restriction effective de la liberté contractuelle de la personne qui fait une demande de carte de crédit restreint aussi sa liberté de détermination à propos de la communication de données requise par le formulaire de demande. On ne peut donc généralement pas partir du principe que la communication des données impliquerait en soi un consentement valide en vue d'une transmission à des tiers (cf. à ce propos la décision de la Commission fédérale de protection des données du 21 novembre 1996, droit de bail, p. 30).
Ce consentement doit être libre et éclairé, et porter sur l'ensemble du traitement. En d'autres termes, la clause de consentement doit être formulée de manière claire et sans équivoque pour que le client reconnaisse le but, la signification et la portée de son consentement. Il doit pouvoir notamment reconnaître les catégories de données, le but du traitement, les catégories des données personnelles traitées et les destinataires (tiers). Même lorsque les données sont communiquées à des filiales, au sein du groupe ou à d'autres entreprises de la même branche, il s'agit toujours de tiers. La communication systématique par exemple de «données négatives» à des tiers tel un organe central ne ressort pas suffisamment clairement des circonstances et à notre avis n'entre pas dans le cadre usuel du rapport contractuel attaché à la carte de crédit. Il faut attirer expressément l'attention du client sur ce service central et ses membres, tout particulièrement lorsque différentes entreprises de cartes de crédit travaillent ensemble. S'il ne dispose pas d'un consentement valide, le service central ne peut justifier l'atteinte et celle-ci demeure illicite. Chaque fois que cela est possible, il faut informer la personne concernée de la durée de la conservation des données et des suites d'un refus de livrer des informations.
Exemple de clause de consentement:

Je confirme par la présente l'exactitude des indications ci-dessus et autorise l'entreprise XY à demander à mon employeur, à ma banque ainsi qu'à l'office des poursuites les renseignements nécessaires à l'examen de la présente demande et à l'utilisation ultérieure de la carte. Par ailleurs, la communication d'informations à des tiers extérieurs est exclue. Sont réservés d'éventuels ordres exécutoires en vue de la transmission des données ainsi qu'une annonce à l'organe central (composé de 90 membres des différents domaines suivants: A, B, C, etc.) en cas de carte bloquée, d'utilisation abusive de la carte ou d'arriéré de paiement qualifié (à partir de trois mois et pour plus de Fr. 2000).

Au cas où des données sont requises dans des buts différents (facturation, publicité, communication à l'organe central en cas de blocage, autres tiers, etc.), il doit être clairement reconnaissable pour le client moyen quelles données sont traitées et dans quels buts. Par exemple on ne peut utiliser des données personnelles à des fins de marketing que si le consentement du client a été obtenu auparavant. Ce consentement sera explicite et distinct (par ex. un encadré à cocher sur le formulaire de demande de la carte). Idéalement, la clause de consentement doit figurer sur la demande de carte de crédit et devrait au moins ressortir visuellement (techniques d'impression). Cela permettrait aussi de répondre aux exigences posées par la directive européenne sur la protection des données qui prévoit que la personne concernée consente en connaissance de cause et sans aucune incertitude.
Les traitements de données personnelles nécessaires à l'exécution d'un contrat peuvent être réglementés dans les conditions générales. En revanche, les traitements de données qui ne sont pas en rapport direct avec l'exécution du contrat comme l'utilisation de données à des fins de marketing interne ou externe ne doivent en aucun cas figurer dans les conditions générales.
Imposer à un client un traitement de données qui n'a rien à voir avec l'exécution directe du contrat ne constitue pas un motif justificatif, ni ne répond au principe de la proportionnalité. Dans ce cas, si le client ne souhaite pas l'utilisation de ses données à des fins de marketing, il est obligé de renoncer aussi à la prestation. Ces traitements de données nécessitent donc une déclaration de consentement séparée de la part du client, déclaration qui ne sera pas couplée aux conditions générales. Refuser de livrer ses données personnelles à des fins de marketing ne doit pas avoir de répercussions négatives sur le reste du déroulement du contrat.

7.2. Publication de listes concernant la solvabilité

Les personnes privées ne doivent pas établir de listes mensuelles sur la solvabilité de débiteurs, ni les communiquer à des tiers ou des membres d'une association. En effet, l'exactitude des données ne peut être garantie. Ce genre de traitement n'est ni proportionnel, ni justifié.

Une poursuite avait été engagée contre une personne privée à la suite d'une créance qui n'avait pas été immédiatement réglée. Le débiteur fit recours et manqua le jour d'audience. La créance fut ensuite immédiatement payée. Un mois plus tard, le nom de la personne concernée figurait dans la revue d'une association sur une liste de personnes considérées comme mauvais payeurs ou insolvables. Il en résulta pour la personne concernée des torts et des dommages considérables, à la suite de quoi elle s'adressa à nous.

Les listes de noms, adresses et données sur des procédures de poursuites pour dettes ou de faillites se rapportent à des personnes déterminées ou déterminables. Bien que cela ne constitue ni des données sensibles, ni des profils de la personnalité, il faut que les principes généraux du traitement des données soient respectés lors du traitement de ces données personnelles. Le titulaire du fichier doit en particulier veiller à ce que les renseignements soient justes.
Le fait que des listes complètes de noms et d'adresses soient communiquées à l'ensemble des membres d'une association se heurte au principe de la proportionnalité (cf. 2ème Rapport d'activités p. 152). Dans un cas d'espèce, il faut certes traiter autant de données que nécessaire, mais aussi peu que possible. Il est évident que chaque membre ne va pas conclure un contrat avec chaque personne de la liste et ne doit donc pas connaître tous les noms. Il est choquant qu'une facture soit payée en mars 1997, après notification de la commination de faillite, et que le nom de la personne concernée paraisse à nouveau en mai sous la rubrique commination de faillite. Cette publication n'est pas proportionnelle. Il peut très bien arriver que par mégarde, une personne consciencieuse ait beaucoup de retard dans le paiement d'une facture. Mais si ses données sont immédiatement consignées sur une liste, cela fait naître une image fausse de la personne concernée. Le principe de l'exactitude ne peut alors pas être respecté. On ne peut exclure qu'entre-temps, la personne concernée subisse des torts et puisse faire valoir une prétention en dommages-intérêts.
Il faut donc examiner si ce genre de traitement repose sur des motifs justificatifs. Dans le cas présent, on ne peut déduire de motifs justificatifs ni du consentement de la personne concernée, ni d'une loi.
Un intérêt privé prépondérant entre en considération lorsque les données personnelles sont traitées pour évaluer la solvabilité d'une autre personne; mais elles ne doivent être ni sensibles ni constitutives de profils de la personnalité et ne doivent être communiquées à des tiers que si ceux-ci en ont besoin pour conclure ou exécuter un contrat avec la personne concernée. Les membres de l'association ne recevront pas seulement les données dont ils ont effectivement besoin pour la conclusion ou l'exécution d'un contrat, mais une liste de débiteurs potentiels. Cette pratique se heurte au principe de la proportionnalité. Le motif justificatif de l'intérêt privé prépondérant ne peut donc pas être retenu.
Il convient aussi d'examiner si un intérêt public prépondérant pourrait justifier une violation de la personnalité. Etant donné l'augmentation de la concurrence économique, on peut admettre un certain intérêt économique à des informations sur la situation financière du partenaire contractuel. Mais dans les relations privées courantes, la plus grande prudence s'impose avant d'admettre une justification de la violation de la personnalité par des intérêts publics prépondérants. Certes il y a un intérêt justifié des membres d'une association à recevoir des informations sur la solvabilité des personnes avec lesquelles ils veulent entrer en relation commerciale. Néanmoins seule la personne pouvant rendre crédible un intérêt peut consulter les procès-verbaux des offices de poursuites et faillites (article 8a, 1er alinéa de la loi fédérale sur la poursuite pour dettes et la faillite, LP). Un intérêt de ce type est notamment rendu vraisemblable lorsque la demande d'extrait est directement liée à la conclusion ou la liquidation d'un contrat (article 8a, 2e alinéa LP). Conformément aux articles 232, 1er alinéa et 268, 4e alinéa LP, l'ouverture et la clôture de la procédure de faillite sont communiquées publiquement par l'office des faillites. Il n'en résulte pas qu'entre l'émission du commandement de payer et l'ouverture de la faillite, d'autres renseignements puissent aussi être rendus accessibles à un grand nombre de personnes ou de membres. De plus, la publication de listes dans une re-

vue ne permet pas aux membres d'examiner leurs intérêts à propos de chaque personne mentionnée. Pour cette raison également, il convient de ne pas admettre d'intérêt public prépondérant.
L'argument selon lequel les données seraient publiées dans un média à caractère périodique ne peut être invoqué à propos des listes mensuelles paraissant dans la revue d'une association. A ce propos, le législateur s'est référé exclusivement à la partie rédactionnelle d'un média à caractère périodique. La notion d'«exclusivement» indique clairement que les données en question ne peuvent être traitées à la fois dans une optique rédactionnelle et commerciale, ce qui ne permet pas non plus de retenir ce motif justificatif.
Il n'y a donc pas en l'espèce de motif justificatif susceptible de légitimer la violation des principes de proportionnalité et d'exactitude des données. La communication de données personnelles en corrélation avec l'examen de la solvabilité ne peut donc avoir lieu que sur demande et au cas par cas (on-line uniquement après introduction d'un nom/critère de recherche précis; cf. à ce propos le 4e rapport d'activités, p. 163).
Afin de garantir l'exactitude des données fournies aux personnes intéressées, la communication illicite par liste de données personnelles a été supprimée. Les données ne sont plus disponibles qu'au moyen d'un système électronique, ainsi leur exactitude est vérifiée en permanence. Les données anciennes et inexactes sont immédiatement rectifiées dans le système.

8. Marketing direct

8.1. Le commerce d'adresses

Marketing direct: telle est aujourd'hui la formule magique de nombreux professionnels de la publicité pour élargir leur clientèle. En des temps de concurrence toujours plus dure, il n'est pas étonnant que l'adresse elle-même soit traitée comme un produit. Fondamentalement, on ne peut rien reprocher à l'utilisation d'adresses à des fins publicitaires. Néanmoins, dans ce domaine aussi, il convient de respecter quelques règles du jeu qui ont trait à la protection des données.

La vente et la location d'adresses constituent un traitement de données personnelles au sens de la loi fédérale sur la protection des données (LPD). Ce traitement doit donc respecter les principes généraux de protection des données (licéité; principes de la bonne foi, de la proportionnalité, de la finalité, ainsi qu'exactitude des données). Ce qui signifie pour l'essentiel:
il est permis d'utiliser des adresses à des fins publicitaires lorsque la personne concernée a rendu son adresse publiquement accessible (par ex. inscription volontaire dans l'annuaire ou dans des recueils professionnels) et n'en a pas interdit l'utilisation à des fins publicitaires. A l'inverse, il n'est pas permis de procéder à un traitement de données contre la volonté de la personne concernée, raison pour laquelle le souhait de faire bloquer son adresse doit dans tous les cas être respecté. Toutes les données sur la personne concernée doivent donc être immédiatement munies dans le fichier d'adresses d'une mention de blocage (par ex. bloquée pour utilisation à des fins publicitaires) et l'effectivité du blocage est à confirmer par écrit à la personne concernée. En cas d'acquisition de fichiers d'adresses, il est recommandé, afin d'éviter d'inutiles réclamations, de comparer ces fichiers avec la

liste Robinson établie par l'Association suisse pour le marketing direct (Case postale, 8708 Männedorf).
En vertu de l'article 8 LPD, toute personne concernée peut demander des renseignements sur toutes les données enregistrées la concernant. La qualité et de ce fait la grande valeur marchande de certains fichiers d'adresses sont dues au fait que diverses entreprises spécialisées dans le commerce d'adresses disposent de données supplémentaires sur les personnes enregistrées dans leurs fichiers. Ces données supplémentaires servent de critères de sélection et permettent une publicité ciblée selon l'âge, le sexe, la profession, la catégorie de pouvoir d'achat, la branche d'activité, etc. Bon nombre de données de ce genre peuvent être obtenues uniquement sur la base du nom et de l'adresse à l'aide de relevés statistiques selon une clé spécialement créée dans une optique de marketing. Ces données aussi doivent être communiquées par écrit dans leur intégralité aux personnes demandant des renseignements.
La collecte d'informations supplémentaires se fait très souvent par sondages d'opinion ou, récemment, par le biais de cartes-clients. Dans les deux cas, on établit ainsi un profil de consommation des personnes concernées qui peut, entre autres, être utilisé pour sélectionner des adresses. Il est donc important que les personnes concernées soient très exactement informées du but du sondage ou du relevé de données par le biais d'une carte-client. Il ne suffit pas de faire état des notions d'étude de marché ou de marketing pour faire comprendre clairement à la personne concernée dans quel but les données relevées seront utilisées. Dans le cas présent, un profil de la personnalité au sens de la LPD étant établi en relation avec le comportement de consommation de la personne concernée, il convient de soumettre à des conditions plus strictes le consentement des personnes concernées en vue du traitement de données personnelles. Ce consentement n'est juridiquement valable que lorsque ces personnes connaissent dans sa totalité la portée du traitement. Le mot marketing peut signifier beaucoup de choses: exploitation du profil de consommation, transmission à des entreprises tierces dans le but de vendre des adresses, de procéder à des envois publicitaires, d'appeler à verser des dons, d'offrir des prestations, etc. Il faut par ailleurs souligner très clairement le fait que la participation à ces sondages est entièrement libre. Dans le cas contraire, on ne peut parler de consentement valable juridiquement (à ce propos, cf. pour plus de détails p. 177).
Les données personnelles ne doivent être traitées que dans le but indiqué lors de leurs collecte. Si ce but est ensuite modifié, on ne peut tout simplement continuer à utiliser les données relevées. Il faut à nouveau demander le consentement des personnes concernées.
Les études de marché effectuées dans l'optique d'une collecte d'adresses sont la plupart du temps orientées vers les informations concernant les ménages en tant qu'unité. En effet, l'efficience d'une publicité directe de qualité se caractérise par une économie de coûts. Voilà pourquoi de nombreux questionnaires d'études de marché s'adressent certes à la personne interrogée elle-même, mais aussi portent sur le comportement de consommation d'autres membres du ménage. Il convient donc de retenir à cet endroit que toute personne concernée ne peut donner de consentement valable juridiquement en vue du traitement de données que pour elle-même. Un questionnaire renferme toutefois la possibilité de faire consigner la clause de consentement par les autres membres majeurs du ménage. Les sondages par téléphone ne doivent toutefois pas contenir de questions qui ne se rapportent pas à l'interlocuteur. Enfin, quiconque qui vend ou loue des adresses doit annoncer son

fichier auprès du Préposé fédéral à la protection des données si la personne concernée n'a pas connaissance du traitement.

8.2. Associations: communication de listes de membres

Nous avons été très souvent consultés pour savoir si dans l'optique de la protection des données, la liste des membres pouvaient être transmises aux membres d'une association. La LPD n'offre malheureusement pas de formule «passe-partout» à ce sujet. Elle établit néanmoins certains principes qui permettent de se prononcer dans chaque cas.

La transmission de la liste des membres aux membres d'une association constitue un traitement de données au sens de la loi fédérale sur la protection des données (LPD). Ce traitement doit respecter les principes de protection des données formulés à l'article 4 LPD (licéité; principes de la bonne foi, de la proportionnalité, finalité et exactitude des données). Quiconque traite des données personnelles ne doit pas porter une atteinte illicite à la personnalité des personnes concernées. Un traitement impliquant une atteinte à la personnalité n'est possible qu'en présence d'un motif justificatif (consentement de la personne concernée, base légale, intérêt prépondérant public ou privé).
Le Code civil suisse (CC) ne contient que peu de dispositions contraignantes dans le domaine du droit des associations. Dans une large mesure, le législateur a laissé à ces dernières le soin de déterminer les compétences des différents organes (statuts). Néanmoins l'article 64, 3e alinéa CC contient à l'encontre du principe de l'autonomie d'association une restriction en matière d'organisation en ce sens: le respect des règles statutaires ne doit pas considérablement entraver l'exercice des droits attachés à la qualité de membre. Cela suppose notamment, lorsqu'une assemblée extraordinaire est convoquée, que chaque sociétaire puisse consulter le fichier des membres afin de pouvoir atteindre les personnes potentiellement unies par les mêmes intérêts, calculer et respecter le quota légal ou statutaire. Sans ce droit de consultation, l'exercice d'un droit impérativement attaché à la qualité de membre serait fortement entravé ou même impossible. Nous estimons donc que du point de vue de la protection des données, rien ne s'oppose à ce que l'on remette aux sociétaires la liste des membres afin de convoquer une assemblée extraordinaire. En l'espèce, la nécessité de présenter un motif justificatif est satisfaite. Pour cette raison, il n'est pas nécessaire de recueillir le consentement de chaque membre de l'association. Par ailleurs, s'il y a violation des droits attachés à la qualité de membre, on peut faire appel au juge conformément à l'article 75 CC.
Afin d'éviter d'éventuels abus (détournement de finalité) ou de satisfaire à la nécessité de transparence imposée par la protection des données lors du traitement de données personnelles, il est indiqué de demander une garantie à chaque membre à qui la liste des membres est remise. Afin de donner du poids à l'interdiction d'abus, on pourrait entre autres envisager aussi une modification des statuts dans ce sens. La LPD ne prévoit pas de prescriptions de forme à ce propos.
Nous soulignerons ici qu'à chaque traitement de données personnelles, il faut à nouveau contrôler le caractère licite du traitement en tenant compte des principes de protection des données mentionnées plus haut. On ne peut donc répondre d'une manière générale par oui ou par non à la question de savoir si chaque sociétaire a le droit de se faire remettre la liste des membres. Cela dépend toujours du but pour lequel la liste est utilisée et si elle est effectivement nécessaire pour atteindre le but

en question. Dans la mesure où il ne s'agit pas comme ci-dessus de l'exercice d'un droit impérativement attaché à la qualité de membre pour lequel la liste des membres est nécessaire, il faut recueillir leur consentement. Il n'est pas nécessaire que chaque membre approuve la publication de la liste en question. Il suffit qu'un droit d'opposition contre la transmission de ses données personnelles soit concédé à chaque membre. La mention de ce droit peut figurer par exemple dans le procès-verbal de l'assemblée générale, qui est envoyé à tous et dans lequel figure un délai approprié pour faire opposition. Pour la transmission de listes d'adresses à des tiers ou à des membres à des fins externes à l'association, un consentement est requis dans la mesure où cette transmission ne repose pas sur un autre motif justificatif. Les considérations figurant plus haut à propos de l'interdiction d'abus sont applicables ici par analogie.

8.3. Marketing international et protection des données

De plus en plus de firmes commerciales suisses et étrangères tentent de créer de nouveaux débouchés en pratiquant une publicité directe transfrontière. Cette tendance a notamment comme corollaire le fait qu'un flot toujours plus grand d'envois publicitaires indésirables remplit nos boîtes aux lettres. Nous cherchons à lutter contre cette situation déplaisante notamment en collaborant à l'étranger avec les autorités locales de protection des données.

Depuis quelque temps, nous sommes de plus en plus consultés par des personnes qui veulent faire valoir leur droit d'accès ou de blocage auprès d'entreprises commerciales présentes au niveau international; ces personnes ne désirent pas de publicité, le font savoir et se heurtent très souvent à un mur car dans ces entreprises, personne ne semble responsable des problèmes de protection des données. Cette situation très regrettable s'explique ainsi: tout d'abord les responsables des entreprises concernées ne sont pas encore conscients de leurs obligations en matière de protection des données; par ailleurs, dans une organisation structurée de manière confuse, personne ne se sent concerné par les affaires relevant de la protection des données. Quelle que soit la manière dont les divers cas se présentent dans les détails, nous retiendrons ici les considérations de protection des données les plus importantes dans ce contexte.
Lorsque la filiale, qui a son siège en Suisse, d'une entreprise étrangère traite des données personnelles, les dispositions de la loi fédérale sur la protection des données (LPD) sont applicables. Cela signifie entre autres que l'on doit communiquer à la personne qui le demande toutes les données enregistrées la concernant. Pour être en mesure de donner des renseignements, il faut donc prendre toutes les mesures organisationnelles qui s'imposent, en premier lieu la désignation d'une personne compétente pour donner les renseignements. Si l'entreprise ne veut pas se plier à l'une ou l'autre des obligations fondamentales en matière de protection des données, le Préposé fédéral à la protection des données peut examiner si le traitement des données personnelles est effectué conformément à la LPD. Tout maître d'un fichier est donc tenu de participer à l'éclaircissement des faits. S'il refuse sa participation ou donne des renseignements faux, il peut se rendre punissable pénalement. Quiconque transmet des données personnelles à des tiers doit en outre annoncer son fichier auprès du Préposé fédéral à la protection des données dans la mesure où les personnes concernées n'en ont pas connaissance ou si le traitement n'est pas soumis à une obligation légale.

Dans les cas où nos démarches ne donnent rien parce qu'au sein de la représentation suisse d'une entreprise étrangère, personne ne semble chargé du traitement des données, nous avons encore la possibilité de prier les autorités étrangères de protection des données, au siège principal de l'entreprise en question, de nous prêter assistance, ce que nous avons fait dans le cas d'une entreprise allemande.

9. Statistique

9.1. Recensement 2000 – un recensement de transition

Au lieu d'abroger comme il est prévu le principe de finalité, le meilleur moyen de rationaliser les procédés de relevé du recensement tout en respectant les principes de protection des données serait de créer une base constitutionnelle dès le recensement 2000. Dans ce sens, le recensement 2000 est une sorte de recensement transitoire qui ne sert qu'à préparer le passage du relevé général par formulaire aux futurs recensements fondés sur les registres.

Après l'adoption le 21 mai 1997 par le Conseil fédéral du message sur le recensement 2000, le Conseil des Etats a suggéré que la loi fédérale sur le recensement (LFR) dans son entier soit révisée dans l'optique d'une loi au contenu transparent. Lors de la séance des 3 et 4 novembre 1997, la Commission de la science, de l'éducation et de la culture s'est prononcée à l'unanimité en faveur d'une révision totale de la LFR sous le nouveau nom de loi fédérale sur le relevé structurel de la Suisse. Le Conseil des Etats a approuvé le projet de révision totale le 17 décembre 1997. Nous nous sommes exprimés sur ce projet ainsi que sur le problème général des futurs relevés indirects.
Ainsi que nous l'avons mentionné dans notre 4e rapport d'activités, nous n'approuvons pas une révision de la loi sur le recensement qui affaiblirait le secret de la statistique et la protection de la personnalité. Toutefois, si une telle révision devait être adoptée, nous avons requis qu'au moins quelques conditions soient remplies pour garantir la protection de la personnalité (cf. à ce propos le 4e rapport d'activités, p. 166). Cette requête a été prise en considération dans le projet du Conseil fédéral. Même la proposition de révision totale de cette loi – exception faite du remplacement de la notion de «recensement» par la notion de «relevé structurel» - prend en considération et même renforce nos exigences (en ce qui concerne l'utilisation de données extraites d'un recensement pour établir un registre fédéral des bâtiments et habitations).
Pour qu'à l'avenir, le recensement puisse être établi à partir des registres, il faudra absolument tenir des registres cantonaux qui servent de support à ce genre de relevé statistique. L'utilisation de données personnelles relevées à des fins statistiques afin de mettre à jour les registres cantonaux et communaux est un procédé peu orthodoxe qui enfreint le principe de la finalité. Cela parce qu'il manque une base constitutionnelle qui donnerait à la Confédération la compétence législative de gérer uniformément le domaine des registres.
Au lieu de l'abrogation désormais prévue du principe de la finalité, la création de cette base constitutionnelle constituerait déjà pour le recensement 2000 la meilleure manière de rationaliser la méthode de relevé du recensement en respectant la protection des données. C'est la raison pour laquelle nous avons souligné dans ce contexte que l'utilisation des données du recensement pour la mise à jour des registres des habitants ainsi que pour la constitution d'un registre fédéral des

bâtiments et des habitations tel qu'il est proposé dans le cadre de la révision totale ne constitue qu'une exception limitée dans le temps au principe de la finalité, jusqu'à ce que la base constitutionnelle pour les prescriptions légales de la Confédération soient créée pour harmoniser les registres cantonaux et communaux. Par ailleurs, nous avons précisé que la loi doit être à nouveau révisée pour le recensement 2010 et que le recensement 2000 peut être considéré comme un recensement transitoire. Ce dernier aura pour seul but de préparer le passage du recensement général par formulaire aux futurs recensements établis à partir des registres.

9.2. Le traitement de données géocodées en conformité avec la protection des données

Les données géocodées sont une somme de diverses données géographiques. Elles contiennent en général des coordonnées des bâtiments (rue, numéro, localité, etc.), mais peuvent contenir aussi d'autres indications à caractère géographique. Nous avons été contactés par l'Office fédéral de la statistique (OFS) qui désirait savoir comment ces données peuvent être utilisées et en particulier à quelles conditions il faut soumettre leur communication.

Lorsque des données géocodées ne contiennent pas de renseignements sur des personnes identifiées ou identifiables, elles sont en général qualifiées de données ne se rapportant pas à des personnes. Si l'on part de ce principe absolu, on ne peut appliquer à la diffusion de données géocodées ni les dispositions de la loi fédérale sur la protection des données (LPD), ni la loi sur la statistique fédérale (LSF) parce que ces dispositions ne règlent que la communication de données personnelles.
La LSF réglemente le traitement des données personnelles relevées à des fins statistiques. Selon cette loi, les données personnelles doivent être anonymisées lorsque le relevé est terminé (cf. article 15 LSF). Par ailleurs, les résultats des relevés doivent être accessibles uniquement sous une forme qui rend impossible toute déduction sur les personnes concernées (cf. article 18 LSF). Enfin, l'article 14 LSF prévoit que les données relevées à des fins statistiques ne peuvent être utilisées à d'autres fins (par ex. industrielles ou économiques) que si une loi fédérale l'autorise expressément.
Les questions décisives sont les suivantes: quand et à quelles conditions des données peuvent-elles être qualifiées d'anonymes, dans quelle mesure et à quelles conditions des données géocodées peuvent-elles être communiquées à des tiers?
Conformément au message du 23 mars 1988 concernant la loi fédérale sur la protection des données, des données peuvent être qualifiées d'anonymes lorsque l'identité des personnes concernées ne peut plus être établie ou seulement si l'on met en œuvre des moyens extraordinaires. Cela s'applique à la publication de résultats statistiques, donc à la communication de données géocodées. En admettant que les données géocodées peuvent être connectées avec des données personnelles sans qu'il soit nécessaire de mettre en œuvre des moyens extraordinaires, la communication de ces données ne doit avoir lieu que dans les conditions énumérées aux articles 14, 15, 16 et 17 LSF.

A ce propos, nous aimerions attirer l'attention sur quelques aspects essentiels du problème des données géocodées:

- étant donné la possibilité de sauvegarder, d'exploiter des informations géocodées et de les connecter avec des données personnelles, les systèmes

d'informations géographiques (GIS) comptent parmi les instruments les plus importants et les plus efficaces pour exploiter et analyser des informations relatives à des personnes.

- La technologie GIS dispose du plus grand potentiel en matière de technologie informatique et permet d'empiéter largement sur la sphère privée de l'individu.

- Il est incontesté que l'individu ne connaît ni le degré de détail des informations, ni les informations qui sont traitées à son propos et communiquées à des tiers.

- Dans le futur, on pourra sans aucun doute accroître considérablement les capacités de recherche dans ces ensembles de données. Les nouvelles possibilités de catégorisation qui en découleront pour les exploitations économiques sont extrêmement vastes.

- Une majorité de citoyens perçoivent probablement la mise en œuvre et l'utilisation de données et de systèmes géocodés comme une atteinte à la sphère privée. Afin d'éviter une réaction excessive de leur part et de ne pas mettre inutilement en danger les investissements déjà réalisés dans les données GIS, il faut dès le début planifier et appliquer des mesures judicieuses visant la protection de la sphère privée.

- Seuls les services officiels (par ex. l'Office fédéral de la statistique) disposent actuellement d'informations géocodées détaillées. Ces informations sont utilisées uniquement à des fins officielles précises (statistiques). Leur communication à des services non officiels les rendraient utilisables à d'autres fins (économiques). La question de la finalité des données se pose donc également dans l'optique de la loi fédérale sur la statistique.

- On peut déjà regrouper et connecter des données géocodées avec d'autres données (dont des données personnelles) sans qu'il soit besoin de mettre en œuvre de grands moyens. A l'avenir, il sera plus facile encore de procéder à toutes sortes de recoupements avec les ensembles de données les plus divers. Déjà utilisée aujourd'hui, la méthode du «cross-matching» est appelée à l'être davantage encore.

- Le destinataire type de données géocodées désire des informations qualifiées (données géocodées) dans une ou plusieurs combinaisons pour certaines régions d'un pays. Ces données peuvent être connectées avec des données d'adresses ou autres données personnelles en fonction de divers critères (par exemple région, rue, canton, langue, etc.). et livrer des informations révélatrices sur l'un ou l'autre groupe de population.

- En général, les données géocodées sont communiquées sans données personnelles. On peut néanmoins faire aisément la liaison avec par exemple les adresses figurant dans l'annuaire (disponible sur le marché sous forme de CD-ROM). Connecté avec des données géocodées, un fichier rassemblant déjà des données (un fichier-clients par ex.) peut livrer des informations révélatrices entre autres sur le comportement en matière de consommation des individus, si l'on vérifie systématiquement les données dans plusieurs

sources de données. De ce fait, dans le secteur privé, les données géocodées peuvent être utilisées en connexion avec des données personnelles en matière de marketing, assurance, banque et immobilier pour ne citer que quelques domaines. Il existe une multitude de possibilités d'utilisation commerciale associées à des données géocodées sans que la personne concernée soit informée et ait donné son accord.

- Il faut donc respecter l'exigence fondamentale de tout traitement licite des données, à savoir l'information et le consentement sans équivoque de la personne concernée en vue du traitement de ses données personnelles.

- Si, durant cette phase préparatoire, on prend des mesures visant la transparence des traitements de données à partir de données GIS, on diminue considérablement le danger de devoir restreindre les utilisations positives des données GIS.

Il est décisif à l'avenir de savoir quelles données peuvent contenir les banques de données dites GIS. On peut résumer ainsi la marche à suivre :
- déterminer de manière exhaustive les données «illicites»
- lorsque les données géocodées sont très détaillées (plusieurs variables), limiter leur but ou accroître l'agrégation des données
- définir de manière exhaustive les buts d'utilisation
- prendre des mesures de sécurité
- garantir les droits des personnes concernées.

Si des données géocodées sont mises à disposition (par ex. sur CD-ROM) ou diffusées, il faudrait pouvoir bloquer la connexion avec des données personnelles.
Une autre possibilité serait, selon le degré de détail des données GIS fournies, de limiter en conséquence les possibilités de connexion. Cela signifierait que plus les données géocodées sont détaillées, plus les possibilités de connexion avec des données personnelles seraient restreintes. Par exemple le Bureau Américain de la Statistique requiert que les données géocodées dont le degré de détail est inférieur à 100'000 personnes ne puissent pas être utilisées à des fins privées.

La solution aux problèmes du traitement de données géocodées dépendra de manière décisive des exploitants de banques de données GIS qui, s'ils garantissent les droits de la personnalité, contribueront à faire accepter la technologie et les banques de données GIS par la population.

II. AUTRES THEMES

1. Cartes-clients

1.1. Le traitement de données personnelles lors de l'utilisation de cartes-clients

- Généralités

Tout rabais accordé repose sur l'intention de lier le plus étroitement possible le client à l'entreprise. A cet égard, la transparence est néanmoins une condition indispensable pour que le consommateur moyen puisse discerner les avantages et inconvénients potentiels d'une carte-client et ensuite se décider librement.

De plus en plus d'entreprises cherchent à améliorer leurs résultats, ce qui est tout à fait légitime. Néanmoins une information transparente et équilibrée doit être à la base de toute réclame pour ce genre de prestations. Nous demandons qu'un détenteur potentiel de carte-client ne puisse pas seulement avoir le choix de dévoiler ses habitudes de consommation au moyen d'une déclaration de consentement. En effet, le client ne doit pas être informé uniquement des divers avantages de la carte-client, mais aussi des traitements auxquels il est envisagé de soumettre ses données de consommation. Il faut indiquer en particulier dans quel contexte ses données seront traitées et si elles seront transmises à des tiers. Si tel est le cas, il faut également indiquer le but d'utilisation.
Ce n'est que lorsque l'information ne porte pas seulement sur les rabais ou autres ristournes, mais aussi sur les traitements envisagés pour les données de consommation que l'on peut parler d'une information claire, équilibrée et correcte vis-à-vis de la clientèle. Par conséquent, le client peut décider librement à propos des avantages et inconvénients d'une carte-client et déterminer si cette dernière présente pour lui un avantage.

- Carte-client M-Cumulus

Le formulaire de demande d'une carte-client doit indiquer clairement quel sera le traitement ultérieur des données fournies afin de permettre au client d'estimer s'il désire ou non ledit traitement. La carte M-Cumulus génère des profils de la personnalité qui peuvent être utilisés à des fins statistiques ou de marketing. Les clients doivent être libres de décider s'ils veulent livrer leurs données à ces fins ou s'ils désirent acheter sans rabais.

La Coopérative Migros nous a prié d'examiner sous l'angle de la protection des données un formulaire de demande, accompagné de conditions générales, pour un nouveau système de rabais. Nous avons fait observer à ce propos qu'au moment où il se procure la carte, le client doit être informé du but du traitement auquel il est prévu de soumettre les données le concernant. Etant donné que seules les données propres à atteindre un but précis et effectivement nécessaires ne devraient être collectées, il suffit de demander le nom, le prénom et l'adresse du client. Nous avons requis que l'indication de la date de naissance, ainsi que la mention des autres membres de la famille vivant au sein du même ménage soient facultatives. Les

personnes majeures qui achètent régulièrement à la Migros ne doivent pas non plus indiquer leur date de naissance à chaque achat.
Or il ressort de la demande de carte M-Cumulus que les données personnelles sont traitées à des fins statistiques et de marketing. Comme il apparaît du reste à la lecture des conditions générales, les données sont ensuite échangées à l'intérieur de l'ensemble du groupe Migros, c'est-à-dire Ex-Libris, les Ecoles-Clubs Migros, les stations-service Migrol, les magasins d'alimentation, etc. D'une part la Migros a ainsi la possibilité d'établir des profils de consommateurs, de les exploiter et d'adresser à ses clients une publicité ciblée. D'autre part, l'accumulation de points, les «bonus», est récompensée par un rabais modeste. Néanmoins, l'attention des clients est attirée sur le traitement auquel il est prévu de soumettre leurs données et ils sont libres d'y consentir. Bien que des profils de la personnalité soient communiqués au sein du groupe Migros (tiers), le consentement de la personne concernée justifie ce traitement de données personnelles. Néanmoins, chacun est libre d'acheter ou non avec une carte M-Cumulus et de livrer le cas échéant des données sur lui-même ou des personnes qui vivent dans le même ménage dans le but d'établir des profils de la personnalité. Si une personne souhaite uniquement la carte M-Cumulus et coche le formulaire en conséquence, ses données ne devraient être utilisées que pour l'octroi du bonus et pour l'exploitation statistique, mais pas à des fins de marketing. Vu que les données ne doivent donc pas être utilisées dans un but de traitement relatif à une personne, les données sur les biens consommés doivent être traitées uniquement de manière anonyme.
Quant aux questions fondamentales soulevées par le traitement de données associées à une carte-client de ce type, nous vous renvoyons au texte précédent (p. 177).
La Fédération des Coopératives Coop remet aussi à ses membres une carte-client qui permet de bénéficier de rabais. Contrairement à la Migros, la Coop ne collecte actuellement pas de données personnelles.

2. Publication de données personnelles

2.1. Publication de noms en relation avec les fonds en déshérence

Avant de publier le nom et le domicile de personnes ayant un lien avec les fonds en déshérence, il faut faire le maximum pour contacter directement les personnes en question. Par ailleurs, dans la mesure où des données peuvent aussi être accessibles sur Internet, une consultation à partir de critères de recherche est indiquée.

En juillet 1997, l'Association suisse des banquiers (ASB) a publié une liste de personnes, rassemblant 1'872 noms et prénoms de clients non suisses, qui avaient ouvert un compte auprès d'une banque suisse avant la fin de la Seconde guerre mondiale. La publication eut lieu dans les principaux quotidiens de 27 pays ainsi que sur Internet.
Or cette liste contenait le nom d'un certain nombre de personnes dont les banques avaient l'adresse ou dont elles auraient pu chercher l'adresse. Par ailleurs, parmi les noms publiés, quelques-uns n'avaient aucun rapport avec les fonds liés à la Shoah ou concernaient des comptes ouverts bien après 1945. Certains survivants de l'Holocauste ainsi que des parents de victimes furent bouleversés de ne pas avoir été informés au préalable par les banques de cette publication et de se voir ainsi

confrontés avec le passé. L'ASB justifia ce procédé par la pression intense qui avaient été exercée sur les trois grandes banques suisses aux Etats-Unis. Une seconde publication de 15'000 à 20'000 ayants droit suisses était prévue pour octobre 1997; à l'occasion d'un entretien entre l'ASB et nous-mêmes, il s'est avéré que les ayants droit suisses dépassaient largement le chiffre de 15'000 à 20'000 noms de personnes ou titulaires de carnets d'épargnes, comptes et dépôts en déshérence.
Nous avons donc recommandé à l'ASB de vérifier l'exactitude des données avant la seconde publication et de comparer les noms de la liste par exemple avec les annuaires électroniques, éventuellement les registres officiels, les annonces déjà parvenues auprès du médiateur des banques et d'Atag Ernst & Young, ainsi qu'avec les adresses d'organisations juives comme le Centre Wiesenthal. Une liste des noms de Suisses et une de non Suisses demeurés introuvables furent ensuite établies sur papier. Ces deux listes étaient disponibles auprès des banques et d'Atag Ernst & Young. Sur Internet, on pouvait consulter non pas la liste complète des ayants droit, mais seulement la liste des personnes étrangères.
Des mesures techniques de sécurité ont permis de protéger les données en particulier contre des traitements non autorisés. En outre, la recherche sur Internet ne pouvait se faire qu'au cas par cas et en fonction de critères de recherche déterminés, par exemple l'indication du nom et de l'adresse. Enfin, à la demande du Congrès juif mondial, la liste des ayants droit non suisses fut aussi publiée dans quelques grands quotidiens étrangers.

3. Législation militaire

3.1. La révision de la législation militaire

Un projet de bases légales destinées au traitement de données par le Département fédéral de la défense, de la protection de la population et des sports (DDPS), notamment pour le traitement de données relatives à la santé, a été élaboré dans le cadre de la révision de la loi fédérale sur l'armée et l'administration militaire (LAAM). Nous avons approuvé le projet de base légale pour le traitement de données relatives à la santé et avons simultanément enjoint au DDPS de réglementer aussi d'autres traitements de données. Fort de l'assurance faite par le Service de renseignements selon laquelle ce dernier ne gère pas de fichiers de données personnelles, nous avons proposé de supprimer sans la remplacer la réglementation d'exception à l'annonce de fichiers auprès du Préposé fédéral à la protection des données dans l'ordonnance relative au Service de renseignements (voir Rapport d'activités 1995/96, p. 184).

Nous avons reçu un projet de base légale formelle pour le traitement des données relatives à la santé au sein du DDPS. Nous l'avons examiné et approuvé. En revanche, le traitement des données médicales des aviateurs ne repose pas sur une base juridique suffisante. Nous avons enjoint au DDPS de créer des bases légales pour le traitement de ces données, mais aussi pour l'engagement des casques jaunes, la protection civile et l'Ecole de sport de Macolin.
Un entretien avec les responsables du service de renseignements a permis d'établir que ce service ne tient pas de fichiers au sens de la LPD. Des données personnelles peuvent exceptionnellement être saisies dans les fichiers d'information du service de renseignements; ils ne font néanmoins pas l'objet de traitement systématique. Nous

avons donc proposé de supprimer entièrement dans l'ordonnance sur le service de renseignements la réglementation d'exception pour l'annonce des fichiers du service des renseignements auprès du Préposé fédéral à la protection des données. Nous avons néanmoins souligné que le service de renseignements, tout comme les autorités de protection de l'Etat, est soumis à la surveillance du préposé. Par ailleurs, nous nous sommes déclarés prêts, au cas où le service de renseignements devrait à l'avenir traiter de manière systématique des données personnelles au sens de la LPD, à utiliser par analogie la réglementation relative à la procédure de déclaration de fichiers de données personnelles traitées dans le cadre de la protection de l'Etat.

4. Archives

4.1. Loi fédérale sur l'archivage

La loi fédérale sur l'archivage présentée par le Conseil fédéral a été débattue aux Chambres fédérales.

La Commission des institutions politiques du Conseil national comme le Conseil des Etats se sont accordés pour fixer le délai de protection pour les données sensibles et les profils de la personnalité à 50 ans à compter de la date du document le plus récent. La commission défend l'opinion selon laquelle une prolongation de ce délai de protection peut avoir lieu en raison d'intérêts prépondérants d'ordre public ou privés. Comme intérêt prépondérant d'ordre privé, la commission retient la sphère intime de la personne concernée. Tous les autres aspects qui selon la LPD sont considérés comme données sensibles, telles des activités religieuses, idéologiques, politiques ou syndicales, la santé et l'appartenance à une race, les mesures d'aide sociale ainsi que les poursuites administratives ou pénales et les sanctions ne constitueraient pas un intérêt privé prépondérant. A notre avis, cette position n'est pas défendable dans l'optique de la protection de la personnalité lorsqu'on considère qu'il est permis, sur la base de cette réglementation, de rendre accessibles au public des données concernant des personnes vivantes, notamment sur leur état de santé, sur d'éventuelles mesures d'aide sociale, sur des poursuites administratives et pénales et sur des sanctions. Une grande partie de ces informations se trouvent par ex. dans les dossiers de l'ensemble du personnel de l'Administration fédérale, qui sont également stockés aux Archives fédérales et pourront être ouverts au public dans 50 ans. Au moment où ces dossiers seront rendus accessibles, toutes les personnes concernées ne seront pas encore décédées.

5. Communication de données personnelles

5.1. Clause de consentement concernant la parution d'annonces dans des services en ligne

La clause de consentement concernant la parution d'annonces dans des services en ligne (notamment sur Internet) à annexer ou insérer dans le contrat entre l'annonceur et la société responsable de la parution de l'annonce s'applique avant tout à des

annonces relatives à des offres d'emploi. Elle peut également être utilisée pour d'autres annonces contenant des données personnelles.

Cette clause de consentement a été élaborée par notre Secrétariat à la demande de plusieurs acteurs du secteur des annonces relatives à des offres d'emploi dans des services en ligne (notamment sur Internet). Elle concerne en premier lieu la communication à l'étranger de données personnelles, notamment dans des Etats n'ayant pas de protection de données équivalente à celle qui est garantie en Suisse. Cette clause vise principalement les contrats entre, d'une part, les annonceurs et, d'autre part, les sociétés de publicité, les éditeurs de journaux ou les sociétés exploitant des services en ligne. Elle peut également être utilisée pour d'autres annonces contenant des données personnelles dans des services en ligne (vente de véhicules, location d'appartements etc.). Cette clause ne couvre cependant que les aspects liés à la protection des données. Elle ne libère pas la société chargée de la parution de sa responsabilité en cas de dommage éventuel dû aux risques inhérents à un service en ligne tel Internet.
Nous avons en outre rappelé aux responsables de la diffusion d'annonces qu'en règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun - c'est le cas pour des annonces - et ne s'est pas opposée formellement au traitement. A ce stade, la société exploitant un service en ligne n'a pas besoin du consentement de la personne concernée et ne doit respecter qu'une opposition formelle à la diffusion de l'annonce. Cependant, la mise à disposition de données sur Internet correspond à une communication de données dans le monde entier, y compris dans des Etats n'ayant pas de protection de données équivalente. Cette situation porte une atteinte illicite à la personnalité à moins d'être justifiée par le consentement de la personne concernée. Pour cette raison, nous avons conseillé aux responsables de sociétés exploitant des sites Internet de demander aux personnes concernées leur consentement. Un modèle de clause de consentement se trouve en annexe du présent rapport voir page 230.

5.2. Remise de données douanières à des entreprises privées pour vérifier la solvabilité?

La remise de données personnelles par la Confédération à des entreprises privées est une opération très délicate pour plusieurs raisons. Déjà la diversité des objectifs commerciaux en présences peut causer des conflits d'intérêts. Quant aux contrôles nécessaires de la part de la Confédération, ils risquent éventuellement d'être en contradiction avec le secret professionnel. Les contribuables qui livrent leurs données sur la base d'une obligation légale ont cependant droit à un traitement des données irréprochable à tous points de vue ainsi qu'à l'existence d'une base légale suffisante.

Conformément aux prescriptions applicables de la législation en matière de taxe sur la valeur ajoutée, l'Administration fédérale des douanes (AFD) est tenue d'accorder de manière générale un délai de paiement de 60 jours aux importateurs et exportateurs soumis à la TVA. Les quelques 14'000 entreprises commerciales concernées possèdent un compte auprès de l'AFD. L'AFD gère les données saisies à l'aide de moyens informatiques propres. Par suite de la situation économique difficile, elle déplore chaque année un manque de recettes qui se monte à plusieurs millions (2 à 3 millions de francs par année). Ces pertes de revenu pourraient être minimisées par un contrôle rapide et efficace de la solvabilité, ce que l'AFD n'est pas

en mesure de faire par ses propres moyens. Pour des raisons de disponibilité et de ressources, l'AFD n'est pas en mesure de mettre sur pied une banque de données pour le contrôle de solvabilité, que ce soit à elle seule ou en collaboration avec d'autres organes fédéraux. L'AFD examine donc la possibilité de mandater une entreprise extérieure spécialisée dans ce domaine pour effectuer ce contrôle de solvabilité. Cette dernière recevrait à cette fin uniquement les données relatives à l'adresse (y compris le numéro d'entreprise et de compte) des entreprises commerciales concernées pour effectuer de manière continue les vérifications et de communiquer immédiatement à l'AFD les éventuelles poursuites ou faillites.
Du point de vue de la protection des données, il faut relever que le traitement de données prévu nécessiterait une base légale au niveau d'une ordonnance. La difficulté principale devrait cependant consister à garantir de manière légalement suffisante que le tiers ne continue pas à traiter les données douanières et fiscales qui lui ont été remises dans un but illicite qui va au-delà de la finalité pour laquelle les données ont initialement été saisies. Les diverses mesures de protection doivent être objectivement appropriées et réglées conjointement avec les responsabilités dans un contrat. La responsabilité principale du traitement correct reste toutefois entre les mains de l'organe fédéral (article 16, 1er alinéa LPD). La mise sur pied d'une expérience pilote avant l'entrée en vigueur d'une ordonnance est délicate du point de vue juridique et devrait en tous les cas dépendre de l'approbation expresse des parties concernées. L'AFD s'est donc immédiatement déclarée prête à effectuer un sondage auprès des entreprises qui entrent en ligne de compte et de soumettre en temps voulu au PFPD, pour prise de position, un contrat d'Outsourcing et des prescriptions de protection des données.

5.3. Communication d'adresses du RCE pour une enquête téléphonique dans le cadre d'un projet de recherche

La communication d'adresses du Registre central des étrangers (RCE) pour établir un échantillon aléatoire pour une enquête téléphonique dans le cadre d'un projet de recherche du Fonds national n'est possible que si les personnes interrogées sont suffisamment informées et si la confidentialité et la sécurité des données sont assurées.

Un institut universitaire a adressé à l'OFE une demande en vue d'obtenir une liste d'adresses de résidants de nationalités turque et italienne. Cette liste devait permettre d'établir un échantillon aléatoire pour une enquête téléphonique réalisée par un institut de sondage dans le cadre d'un projet du Fonds national suisse de la recherche scientifique. Consulté par l'OFE, nous avons autorisé la communication, moyennant les charges suivantes:

- engagement du chercheur à utiliser les données communiquées uniquement pour établir l'échantillon nécessaire à l'enquête téléphonique et à la recherche des numéros de téléphone;
- destruction des données dès que l'enquête téléphonique est effectuée, soit au plus tard trois mois après la communication; le chercheur informe l'OFE de la destruction;
- conservation des données sous clefs et de manière séparée des autres données personnelles;
- limitation de l'accès au chercheur et à son assistant;

- transmission par le chercheur, à l'institut de sondage retenu uniquement, de la liste des numéros de téléphone, sans le nom ou toute autre donnée personnelle relative aux personnes figurant dans l'échantillon;
- engagement du chercheur à veiller à ce que l'institut de sondage ne collecte et ne conserve pas de données personnelles permettant d'identifier les personnes interrogées, à l'exception des données relatives aux personnes acceptant de participer à une prise de contact personnelle; dans ce dernier cas, les données d'identification doivent être conservées séparément des autres données de l'enquête et détruites une fois l'entretien effectué. Les numéros de téléphones doivent également être détruits dès l'entretien téléphonique réalisé;
- engagement du chercheur à veiller à ce que l'institut de sondage informe clairement les personnes interrogées sur les finalités de l'enquête, l'organisme pour le compte duquel l'enquête est effectuée, le caractère facultatif des réponses, l'utilisation des données de manière confidentielle, anonyme et uniquement à des fins statistiques ou de recherche.

6. Protection des données et conditions légales cadres

6.1. Adaptation de lois fédérales à la loi sur la protection des données: quelques exemples intéressants

Les fichiers contenant des données personnelles sensibles ou des profils de la personnalité ne devraient pouvoir être encore utilisés après le 1er juillet 1998, que si une loi au sens formel ne l'autorise de manière explicite. C'est ce qu'exige la loi sur la protection des données. Bien que le nombre de ces fichiers est élevé et qu'il a même augmenté ces dernières années, seul un nombre limité de bases légales ont été adaptées. Les adaptations effectuées sont à vrai dire de bonne qualité, mais il existe néanmoins une grosse lacune. Il s'agit maintenant d'adapter de manière urgente les autres lois. Etant donné qu'il existe de bons modèles, ceci ne devrait pas poser de problèmes insurmontables.

Dans un avis publié dans la JAAC 60.77, dans une circulaire à tous les départements et offices fédéraux ainsi que dans les deux derniers rapports d'activités (1996/97 p. 184, 1995/96 p. 171), nous avions déjà rendu attentif à ce problème. La loi sur la protection des données exige que 5 ans après son entrée en vigueur les fichiers contenant des données personnelles sensibles ne peuvent être encore utilisés que si une loi au sens formel l'autorise expressément. Ce délai est échu au 1er juillet 1998. Nous avons eu l'occasion récemment de juger différents projets législatifs intéressants qui ont bien transposé cette importante exigence de la protection des données. Il sont en partie déjà entrés en vigueur ou le seront dans un avenir proche. Les fichiers et traitements de données ainsi réglementés sont donc licites. Cependant, pour la grande majorité des fichiers contenant des données sensibles ainsi que pour les traitements de données qui s'y rapportent, il n'existe pas de bases légales. De plus, ces dernières n'ont dans certains cas même pas encore été planifiées. Ces fichiers ainsi que les traitements de données qui s'y rapportent doivent donc être qualifiés d'illicites. Il est impératif de remédier d'urgence à cette situation. C'est pour cette raison que le Conseil fédéral a mandaté la Chancellerie fédérale ainsi que les départements de lui remettre un inventaire de l'état des travaux d'adaptation ainsi qu'un plan pour la création rapide des bases légales

faisant défaut. Un «message commun» contenant les modifications nécessaires doit être élaboré cette année encore. Le Conseil des Etats a accepté une initiative de sa Commission des affaires juridiques sous forme d'un arrêté fédéral urgent prolongeant de manière générale la période transitoire de 5 ans. L'objectif doit être qu'à la fin de l'an 2000 les exigences de la loi sur la protection des données soient remplies au moins sur le plan matériel. Ceci devrait être possible étant donné que les services retardataires peuvent aujourd'hui s'appuyer sur de très bons modèles. Ainsi, des fichiers ou traitements de données volumineux ont par exemple été réglementés dans les domaines militaire ou de la législation en matière d'asile et des étrangers (voir aussi p. 125 ss). Pour des traitements d'envergure moyenne, nous avons par exemple soumis des propositions dans les domaines douanier, de l'aviation, de l'énergie ou de la TVA, propositions qui, à l'exception du domaine douanier, ont déjà été transposées. Dans le paquet «Coordination et simplification des procédures – VKB-2» nous avons pu insérer dans les lois dans lesquels cela était nécessaire les dispositions relatives à la protection des données. Il s'agit en l'occurrence de traitements de données clairs qui se prêtent bien à une législation commune sous forme d'un «message commun». De gros efforts doivent encore être entrepris à notre avis dans le domaine de la législation sur le personnel de la Confédération et du droit des assurances sociales. On peut prévoir aussi qu'il reste des adaptations à faire dans les domaines du droit fiscal et douanier, de l'économie extérieure et de l'agriculture ainsi que dans les secteurs d'activités du Département fédéral des affaires étrangères. L'énumération est loin d'être complète. L'Administration des douanes ainsi que le DFAE nous ont désormais présenté des avant-projets pour prise de position. Dans le cadre de notre mandat légal, nous conseillons les organes fédéraux qui s'adressent à nous. Ces derniers doivent cependant prendre l'initiative de nous contacter.

6.2. Implication du PFPD dans le processus de législation

Dans la procédure de législation fédérale, le PFPD doit être impliqué aussi bien lors de la consultation des offices que dans la procédure de corapport. Nous rencontrons deux types distincts de problèmes dans ce domaine. Soit le PFPD n'est pas consulté du tout ou seulement dans une phase préliminaire, ou alors ses remarques sont tout simplement tues dans la suite de la procédure. Nous nous permettrons de décrire le premier type à l'aide d'exemples tirés du domaine de l'assurance sociale et des télécommunications.

Conformément à l'ordonnance relative à la loi sur la protection des données, les offices fédéraux doivent soumettre au Préposé fédéral à la protection des données tous les projets de lois qui concernent un traitement de données personnelles ou qui touchent à la protection des données. A l'occasion de révisions des ordonnances dans le domaine de l'assurance maladie (OAMal et OPAS), nous avons constaté que l'on nous soumet régulièrement les projets de révision de l'OAMal, mais pas ceux de l'OPAS. Il semble bien que ceci ait été motivé par le fait que l'OPAS n'est qu'une simple ordonnance de département qui se borne à définir un catalogue des prestations légales obligatoires, et qui semblait à ce titre ne pas revêtir d'importance au niveau de la protection des données. Nous ne sommes pas entrés en matière, raison pour laquelle la dernière constatation n'est que partiellement pertinente. Par contre, nous avons insisté sur le fait que l'une des nouvelles révisions de l'OPAS (révision du 3 juillet 1997, RO 1997 p. 2039 ss) touchait bien la protection de données. Une des dispositions révisées concerne par exemple les informations que

les assureurs sont en droit de demander. La formulation choisie laisse une grande marge d'interprétation quant au contenu des informations, sans compter qu'elle ne précise pas qui doit collecter ces informations. On peut en déduire pour les deux points que ceci est dû au fait que le PFPD n'a pas été consulté dans le cadre de la révision. Dans l'intervalle, l'OFAS nous a assuré que nous serons dorénavant consultés pour tous les projets de lois qui pourraient concerner la protection des données.
Le cas des travaux préparatifs pour la nouvelle ordonnance relative à la loi sur les télécommunications fut quant à lui très différent. Le PFPD fut bien invité à prendre position dans le cadre de la consultation des offices. Toutefois, des dispositions significatives du point de vue de la protection des données ont été introduites au stade de la procédure de corapport seulement, et ce sans nous informer, ni nous permettre de nous prononcer. Nous sommes intervenus auprès du DFJP et du DETEC pour connaître les raisons de cette omission, ainsi que la provenance des dispositions proposées et les motifs de leur introduction. Répondant au nom des deux départements concernés, le DFJP a invoqué le secret de fonction et refusé de répondre à nos questions. Il a en outre argué du fait que nous pouvions certes intervenir dans la procédure de consultation des offices, mais pas au niveau du corapport, cette procédure étant réservée à des magistrats. Or, il convient de rappeler qu'aux termes de la LPD, le préposé doit se prononcer sur les projets législatifs fédéraux qui touchent de manière importante à la protection des données. Il donne en règle générale son avis dans le cadre des procédures de consultation des offices. Mais si des modifications sont introduites ultérieurement, notamment au niveau du corapport, le préposé doit en être informé et avoir la possibilité de faire valoir son point de vue. C'est au département compétent de rechercher l'avis du préposé. En outre, lorsque dans le cadre de la procédure de consultation, des divergences subsistent, celles-ci doivent être portées par les offices à la connaissance de leur secrétariat général, afin que ce dernier puisse en faire état dans la procédure de corapport. L'avis du préposé doit dans tous les cas être joint à la proposition au Conseil fédéral, afin que ce dernier puisse décider en connaissance de cause. Celui-ci a d'ailleurs reconnu l'importance de cette information, puisqu'en 1995 déjà, deux Conseillers fédéraux, le Chancelier de la Confédération et le préposé ont convenu de la procédure décrite ci-dessus. Ceci également pour des raisons d'économie de procédure, le Conseil fédéral ayant de la sorte une meilleure vue d'ensemble que s'il devait encore prendre connaissance d'un rapport séparé du préposé.

En résumé, on peut présumer que si la non-implication du PFPD s'explique dans nombre de cas par l'inadvertance, la surcharge, le manque de temps ou la négligence, elle est parfois aussi le résultat de motivations – pour l'exprimer de manière modérée – bien moins excusables.

7. Flux transfrontières

7.1. Protection des données équivalente et portée des conventions contractuelles en cas de communications de données à l'étranger

Les communications de données personnelles à l'étranger ne sont en principe autorisées que lorsque la personnalité des personnes concernés ne s'en trouve pas

gravement menacée. La loi fédérale sur la protection des données ne mentionne qu'un élément - l'absence d'une protection des données équivalente à celle qui est garantie en Suisse - qui pourrait gravement menacer la personnalité des personnes concernées.

Durant l'année écoulée, nous avons reçu à plusieurs reprises des demandes de renseignements sur la communication de données à l'étranger. Les questions portaient surtout sur la relation entre l'équivalence des dispositions de protection des données dans le pays destinataire et la nécessité d'une convention contractuelle avec le destinataire des données. En vertu de l'article 6 LPD, la communication à l'étranger de données personnelles ne doit pas gravement menacer la personnalité des personnes concernées. Le législateur n'a mentionné qu'un seul exemple à l'article 6 LPD, à savoir l'absence d'une protection des données équivalente dans le pays destinataire. On ne doit toutefois pas supposer d'une manière générale que l'existence de dispositions de protection des données équivalentes dans le pays destinataire exclue toute violation de la personnalité et que la personne qui communique les données n'a donc rien à entreprendre afin de se conformer à sa responsabilité initiale vis-à-vis des personnes concernées. En effet, même si le pays destinataire possède des dispositions de protection des données équivalentes, on ne peut exclure la possibilité d'une violation de la personnalité, notamment lorsque les droits de l'homme y sont bafoués ou lorsque l'instabilité politico-sociale accroît les risques de violation de la personnalité. Cela mis à part, il est tout à fait possible que du fait de l'organisation interne de l'entreprise du destinataire, on ne puisse exclure un traitement contraire à la protection des données. C'est pourquoi, indépendamment du fait de savoir si une protection des données équivalente est garantie, mais dans la mesure où il règne une incertitude sur la protection de la personnalité (par exemple lorsque le but du traitement des données est peu clair ou équivoque), il est recommandé de conclure une convention ou un contrat avec le destinataire des données. La personnalité des individus concernés s'en trouve ainsi protégée plus efficacement et la personne qui communique ces données assume sa responsabilité initiale.
Le contrat ou la convention peut s'inspirer des clauses modèles du contrat-type du Conseil de l'Europe relatif à la garantie d'une protection des données équivalente. Il convient néanmoins d'intégrer au contrat au moins les éléments suivants:

- utilisation des données personnelles communiquées uniquement dans le but convenu
- garantie des droits des personnes concernées, notamment le droit d'accès et de rectification
- refus de communiquer les données à des tiers
- garantie de la sécurité des données en fonction de leur sensibilité
- établissement d'une peine conventionnelle ou d'une obligation à dommages-intérêts pour le cas où le destinataire ne remplit pas ses obligations.

Dans ce contexte, il ne convient pas de mettre en relation directe l'information ou l'obligation de déclarer une communication à l'étranger conformément à l'article 6, 2e alinéa LPD avec la convention contractuelle. Mettre au courant les personnes concernées ou déclarer le fichier conformément à l'article 6, 2e alinéa LPD ne garantit pas le caractère légal de la communication à l'étranger. Le maître du fichier n'est donc pas libéré de sa responsabilité de veiller au respect de la protection des

données. Indépendamment de cela, il doit vérifier si le traitement des données, pour qu'il soit licite, requiert un contrat.

8. Protection et sécurité des données

8.1. L'utilisation des procédés cryptographiques

- La controverse à propos de la cryptographie

La mise en œuvre de procédés cryptographiques dans notre société d'information actuelle a pour but de protéger de manière efficace la confidentialité, l'authenticité et l'intégrité des informations transmises électroniquement. Le monde des affaires n'est pas le seul a avoir besoin de transmettre des données en toute sécurité. Tout un chacun a le droit de ne rendre des données accessibles qu'aux destinataires qu'il a choisis. Le citoyen peut ainsi préserver le droit de confidentialité garanti par la LPD en mettant en œuvre des procédés cryptographiques.

Grâce aux techniques de communication modernes, tout un chacun peut communiquer sans que son message soit lu ou écouté. Dans de nombreux cas, la cryptographie est le moyen le plus efficace et le meilleur marché de protéger la sphère privée. Pour cette raison, le débat sur le contrôle ou l'interdiction de la cryptographie concerne aussi le droit fondamental à la protection de la sphère privée. Or le fait que les services de l'Etat désirent maintenant lire ou écouter ce genre de communications - contrairement aux communications usuelles (lettres, téléphone) - a déclenché au niveau mondial un débat sur la cryptographie. Pour cette raison, des tentatives ont été faites pour réglementer son usage et permettre aux autorités étatiques d'accéder aux clés de chiffrage (key escrow).
Une réglementation (par ex. utilisation exclusive de chiffrages faibles) compromettrait néanmoins l'utilisation de la cryptographie. En effet, on ne peut aujourd'hui empêcher totalement le chiffrage des données. Il est improbable que l'on puisse contrôler efficacement les infractions qui ont fait l'objet d'un chiffrage en réglementant celui-ci. S'ajoute à cela le fait que grâce aux méthodes stéganographiques, il est impossible de prouver qu'il y a eu échange d'informations. Ces méthodes permettent de dissimuler des données dans d'autres données, par exemple dans des images ou des fichiers sonores. On ne peut ensuite prouver que des informations ont été échangées, et encore moins qu'un procédé de chiffrage (éventuellement illégal) a été utilisé.

En ayant accès à la clé de chiffrage (lawfull access), les autorités peuvent décrypter le message chiffré. Pour les autorités de poursuite pénale, les systèmes d'accès aux clés sont donc une solution permettant de venir à bout des informations chiffrées. Ces systèmes présentent néanmoins un certain nombre de faiblesses. D'une part l'utilisation de la cryptographie dans le but de garantir la protection des données ne peut être restreinte parce que la cryptographie est le meilleur moyen de transmettre des données personnelles en toute sécurité. D'autre part, le secteur industriel fait des réserves considérables à propos du rapport coût/efficacité de l'exploitation de ces systèmes. Enfin, il est très douteux qu'une telle réglementation permette de lutter contre la criminalité. En effet, on ne peut empêcher que des criminels utilisent des procédés cryptographiques efficaces ou esquivent le dépôt des clés de chiffrage. Ainsi une réglementation de l'usage de la cryptographie ou le dépôt des

clés concernerait en premier lieu ceux qui utilisent la longueur de clé autorisée ou déposent leurs clés dans les formes prescrites. Par contre, informés de la réglementation, les professionnels du crime (on peut supposer que les membres du crime organisé disposent d'un niveau d'intelligence moyen) utiliseront d'autres techniques de chiffrage que l'Etat ne peut pas contrôler.
Nous estimons que la réglementation des procédés cryptographiques n'est pas le moyen permettant d'atteindre le but visé. L'atteinte aux droits personnels qu'elle impliquerait est disproportionnée. Nous nous prononçons contre une réglementation ou une limitation de la cryptographie parce qu'elle est impropre à soutenir la lutte contre le crime organisé et menace inutilement la protection des données relatives aux personnes et la protection du secret professionnel et commercial.

- La génération de clés et la sécurité lors de transmissions de données cryptées

Les risques pour une communication cryptée sûre ne viennent pas seulement des tendances à la réglementation citées plus haut. Le procédé concret de génération et de distribution des clés doit être conçu de manière à ce que les clés privées ne puissent pas tomber entre les mains de personnes non autorisées. Car la sécurité d'un système de cryptage ne pourra jamais être meilleure que le secret auquel sont soumis les clés (privées).

Il existe malheureusement des systèmes de communication basés sur des algorithmes asymétriques (systèmes de messagerie par ex.) qui prévoient uniquement une génération centralisée des clés. Cela signifie que la paire de clés nécessaire (clé publique et clé privée correspondante) est générée en un endroit centralisé au lieu de l'être par l'utilisateur lui-même. La clé privée doit cependant être entièrement sous le contrôle de l'utilisateur, sans quoi ce dernier ne pourra jamais avoir l'assurance qu'aucun tiers n'est en possession de sa clé privée, ce qui permettrait à ce dernier de lire son courrier et également d'en envoyer à son nom. Cette assurance ne peut être donnée dans le cas d'une génération centralisée. Il faut donc veiller, lors de la conception ou de l'achat de systèmes de communication, à ce que la génération des clés par l'utilisateur lui-même ne soit pas a priori exclue. Il est pensable qu'il soit nécessaire pour une entreprise ou un service administratif de consigner les clés privées de ses collaborateurs auprès d'un organe de confiance, afin de pouvoir en cas de besoin accéder à des documents professionnels. En ce qui concerne sa communication purement personnelle, l'utilisateur ferait bien dans son propre intérêt non seulement de générer lui-même sa paire de clés, mais aussi d'éviter que des copies de ses «clés privées» soient consignées quelque part.

8.2. Le règlement de traitement du système PISEDI

Si certaines conditions sont remplies lors de la conception de systèmes d'information automatisés dans l'administration fédérale, les dispositions légales exigent qu'un règlement de traitement soit élaboré. Si un tel règlement n'existe pas avant la mise en service du système, ceci constitue une violation des dispositions légales en vigueur.

Selon l'article 21 OLPD, un règlement de traitement doit entre autres être élaboré lors du traitement de données sensibles ou de profils de la personnalité.
Le Secrétariat général du Département fédéral de l'intérieur (SG DFI) a présenté en décembre 1996 à la conférence informatique de la Confédération (CIC) le système

de gestion du personnel du DFI (PISEDI) comme solution transitoire possible pour remplacer le projet BV-PLUS qui avait été stoppé. Le SG DFI a cependant déclaré que le Préposé fédéral à la protection des données (PFPD) était informé du projet et que le système PISEDI pouvait être considéré comme étant conforme à la protection des données. L'étude du dossier PISEDI qui fut faite ensuite auprès du PFPD fit apparaître que plusieurs questions ouvertes relatives à la protection des données n'avaient pas reçu de réponses jusqu'à cette date.
En janvier 1997, le SG DFI organisa une démonstration du système PISEDI, notamment pour des représentants des services du personnel et des informaticiens de l'administration fédérale. Il fut déclaré à l'occasion de cette démonstration que le système répondait aux exigences de la protection des données. Au vu de la situation relatée, le PFPD fut amené à informer le SG DFI, de même que les services intéressés par le système PISEDI que la protection des données n'était pas suffisamment prise en considération. Dans une lettre du 19 mars 1997, nous relevions notamment que ce système ne satisfaisait pas aux exigences de la protection des données et qu'il y avait lieu de contacter le PFPD avant de prendre une éventuelle décision en faveur d'une mise en service du système PISEDI dans les diverses unités. On fit remarquer en outre qu'un règlement de traitement devait être élaboré avant et non pas après la mise en service d'un système de gestion du personnel. Etant donné que PISEDI était, entre autres, déjà en service auprès du SG DFI et qu'il n'existait pas de règlement de traitement, nous avons invité le SG DFI, dans une recommandation fondée sur l'article 27 LPD, à élaborer dans un délai imparti un règlement de traitement pour le système de gestion du personnel PISEDI.
La recommandation a été acceptée par le SG DFI et eut pour première conséquence que l'informaticien du département ne dut plus assumer simultanément la fonction de conseiller en matière de protection des données, mais que cette tâche fut alors confiée à une autre unité au sein du DFI. Cette décision doit être saluée, car il n'est pas pensable que les fonctions d'informaticien de département et de conseiller en matière de protection des données soit assumée par la même personne. Des conflits d'intérêts entre la direction informatique et la protection des données sont évidentes, car le conseiller en matière de protection des données doit veiller à ce que les conditions légales soient respectées dans une mesure adéquate lors de la conception du système informatique.

8.3. Exigences envers un règlement de traitement

Les exigences devant être respectées lors de l'élaboration d'un règlement de traitement sont spécifiques à un système, c'est pourquoi elles ne peuvent pas être fixées sous forme de «livre de recettes». Le législateur a défini ce qu'un règlement de traitement doit contenir. Quant à la forme de sa présentation, il se borne, pour des raisons compréhensibles, à mentionner que les indications doivent être compréhensibles, donc transparentes et reproductibles.

Autant l'article 21 de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) que le guide relatif aux mesures techniques et organisationnelles esquissent les prescriptions pour l'élaboration d'un règlement de traitement. Selon eux, un règlement de traitement doit contenir les éléments suivants:
sur le principe, le règlement de traitement fixe que l'organe responsable doit documenter les parties de l'organisation (organisation fonctionnelle et structurelle) touchées par le système traitant les données. Il doit faire de même pour les procédures de traitement et de contrôle des données. Ici, le législateur distingue

deux types de procédures ou de déroulements. D'une part, il demande de documenter les déroulements ou processus lors du traitement des données et de l'accomplissement de la tâche; d'autre part il demande aussi que les processus de contrôle soient mentionnés. Les processus mis en œuvre pour accomplir la tâche devraient en principe être documentés avant la conception informatique. A cet égard, il faut cependant constater quelques lacunes dans l'administration fédérale. Dans l'optique de la protection des données, les processus de contrôle devraient également être documentés.

Les procédures de traitement des données doivent être documentées. Le terme «traitement» a été défini dans la loi sur la protection des données comme toute opération relative à des données personnelles, quels que soient les moyens et procédés utilisés, notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données. Ce terme est vaste, il débute à la collecte des données et ne se termine qu'une fois les données détruites. Tous les déroulements ayant lieu entre deux doivent être documentés. Plus le traitement est sensible, plus les processus doivent être décrits en détail. Le règlement de traitement doit en outre mentionner les modalités d'exercice du droit d'accès. Les procédures de rectification (mention) et de blocage sont dérivées du droit d'accès. Une destruction des données peut également devenir nécessaire sur la base du droit d'accès. C'est pourquoi ce processus doit également être mentionné.

Les points suivants peuvent être mentionnés sous le terme «sécurité des données»:

- les procédures de contrôle, avec notamment les mesures techniques et organisationnelles selon l'article 20 OLPD;
- la description des champs de données et des unités qui y ont accès;
- le type et la portée de l'accès que les utilisateurs ont au fichier;
- la configuration des moyens informatiques.

Quant aux bases pour l'application des mesures techniques et organisationnelles de sécurité des données dans l'administration fédérale, nous renvoyons au manuel n° 1 relatif à la directive sur la sécurité informatique n° S02 de la section sécurité de l'Office fédéral de l'informatique. Ce manuel contient entre autres un catalogue de mesures pour la transposition des mesures de sécurité des données.

- Il importe en outre dans l'optique de la protection des données de pouvoir constater la provenance des données et le but de leur traitement.
- Le règlement doit en outre mentionner les unités responsables de la protection et de la sécurité des données.
- Les documents de planification et de réalisation d'un système informatique doivent, dans l'Administration fédérale, être établis selon la procédure HERMES (conduite et déroulement de projets informatiques).
- La documentation de l'exploitation doit être contenue dans le manuel d'exploitation.
- Les annonces de fichiers gérés par les diverses unités de l'organisation doivent également être mentionnées dans le règlement de traitement.

Il n'est cependant pas prévu que le règlement de traitement contienne tous les documents qui doivent être élaborés selon la procédure HERMES, mais des déclarations fondamentales dans l'optique de la protection et de la sécurité des données qui découlent des documents déjà élaborés. Il doit en outre renvoyer aux documents déjà créés. Les exigences spécifiques à la protection et à la sécurité des données qui ne sont documentées nulle part doivent être contenues intégralement dans le règlement de traitement.

La première version du règlement de traitement doit être disponible dès que les phases de planification du projet ont été parcourues. Il sera par la suite mis à jour et mis à disposition des organes de contrôle compétents sous une forme compréhensible.

8.4. Journalisation de traitements de données

Une journalisation permet de constater après coup d'éventuels traitements illicites de données, en particulier des transmissions de données, puis de les éviter à l'avenir.

Souvent, les mesures techniques et organisationnelles ne suffisent pas à prévenir des traitements illicites de données. Ceci provient du fait qu'il n'est pas possible de configurer un système informatique dès le départ de manière à ce qu'il n'autorise vraiment que les opérations qui correspondent à la tâche d'un collaborateur, donc qu'il empêche un traitement ne correspondant pas à la finalité annoncée.
La journalisation des traitements de données, à savoir l'enregistrement des opérations de traitement, peut dans de tels cas apporter une solution.
Il y a lieu, lors d'une journalisation, de respecter le principe de la proportionnalité: on enregistrera uniquement les opérations pour lesquelles on s'attend à ce qu'elles permettent un contrôle efficace. Dépendant de l'environnement concret et de la sensibilité, la gamme des mesures s'étend d'une journalisation restreinte par sondages, à l'enregistrement intégral de toutes les activités, avec toutes les nuances possibles entre-deux. Il est aussi envisageable que les traitements ne soient journalisés que s'ils apparaissent délicats sur la base d'une analyse de plausibilité (automatisée). Une journalisation d'un nombre trop élevé d'opérations génère d'énormes volumes de données qui sont très difficiles à dépouiller. Une telle démarche présenterait en outre le risque d'un contrôle du comportement des collaborateurs, ce qui serait en contradiction avec la protection des données.
Lors du traitement automatisé de données sensibles et de profils de la personnalité, une journalisation doit cependant toujours être faite dans les cas où il n'est pas possible a posteriori de constater si les données ont été traitées conformément à leur finalité. Il est essentiel que les procès-verbaux de journalisation soient structurés de manière conforme aux exigences de la révision. Ils ne doivent donc pas pouvoir être manipulés, sans quoi tout l'effort entrepris perdrait sa justification. On peut par exemple envisager l'utilisation de disques optiques du type WORM, mais il est aussi pensable d'imprimer sur papier des documents que l'on conservera en un endroit sûr. Les procès-verbaux doivent être gardés en un endroit sûr et ne doivent être accessibles qu'aux personnes chargées de vérifier l'application des dispositions de protection des données. Toute utilisation allant au-delà de ce but n'est pas admissible. Les personnes qui utilisent le système d'information doivent savoir quels traitements sont journalisés et dans quelle mesure. Le fait de savoir que des traitements de données sensibles peuvent être constatés a posteriori réduit le risque d'opérations illicites. Dans ce sens, l'existence d'une journalisation a – à elle seule déjà – un effet préventif sur le traitement illicite de données personnelles.
En résumé, nous pouvons dire ce qui suit: la question de savoir s'il y a lieu de procéder à une journalisation ou non doit être décidée sur la base d'une analyse des risques effectuée sur des cas concrets de traitements de données. L'aspect décisif est que des données ou traitements de données sensibles ne peuvent pas être protégés par des mesures préventives. Quant au niveau de détail de la jour-

nalisation, il découle également de la situation existante au niveau du traitement de données.

8.5. Outsourcing de prestations informatiques dans l'administration fédérale

Lors de l'attribution de prestations informatiques à des sociétés externes, une attention suffisante doit être vouée à la protection des données. Lors d'un traitement de données personnelles sensibles, les mesures de sécurité des données devant être prises doivent être appliquées en tenant compte du progrès technique. Lors d'une évaluation, il va de soi que les mesures de sécurité dans un environnement sensible doivent recevoir une attention adaptée à la situation.

Un relevé effectué par le centre de calcul de l'Office fédéral de l'informatique a révélé que la durée pendant laquelle une application peut être hors service ne peut pas dépasser 3 jours pour certaines d'entre elles. La configuration actuelle du système ne peut pas garantir cette durée de panne maximale dans les cas graves. On a donc lancé un projet dans le but de déterminer comment ces exigences peuvent être remplies. Malheureusement, la demande de projet n'a pas été – tel que cela est prescrit au sein de l'administration fédérale – remise au Préposé fédéral à la protection des données, ce qui signifie que nous n'avons pas été impliqués dès le début dans les phases de planification. Nous avons néanmoins été informés du projet et avons demandé aux organes responsables de nous remettre les documents nécessaires. En étudiant cette documentation, nous avons pu constater que, lors de l'évaluation du centre de calcul de secours, une attention insuffisante avait été portée en particulier à la confidentialité des informations. Selon les exigences légales de tels systèmes, en raison notamment de la sensibilité des données qu'ils traitent, doivent être protégés en utilisant les possibilités technologiques existantes. Suite à l'évaluation, on choisira finalement entre un fournisseur externe et un fournisseur interne à la Confédération. En principe, rien n'empêche qu'un traitement de données sensibles (traitement de données personnelles sensibles ou de profils de la personnalité) soit confié à l'extérieur, pour autant que le système soit exploité de manière à ce que les données personnelles ne puissent pas être consultées par l'exploitant du centre de calcul. Dans le contexte dont nous parlons, ceci ne pouvait selon nos informations pas être garanti. Une isolation complète des données personnelles dans la mesure exigée n'est aujourd'hui possible qu'à l'aide de procédés de cryptage. Dans le cas précis, nous n'avons cependant pas connaissance de tels procédés. Dans le cas d'un Outsourcing, la responsabilité pour la protection et la sécurité des données incombe au mandant. Ce dernier doit veiller à ce qu'il soit encore en mesure d'exercer le contrôle sur le traitement des données même si des parties de ce dernier sont confiés à des tiers. Ceci est d'autant plus le cas lorsque les données traitées à l'extérieur sont des données sensibles. Des engagements écrits à respecter les prescriptions de protection ou de sécurité des données, tels qu'on en trouve fréquemment, sont des moyens de rendre attentif à la sensibilité du traitement des données. De nos jours cependant, de telles mesures ne peuvent plus être considérées comme suffisantes. L'observation des mesures de protection et de sécurité des données doit être mesurable pour que ces mesures soient contrôlables.

Afin de pouvoir comparer les mesures de sécurité du centre de calcul du fournisseur externe avec celles du centre de calcul de l'administration fédérale, nous avons prié l'Office fédéral de l'informatique de nous remettre une analyse complète de sécurité et de risque pour les deux centres de calcul de secours qui entraient en ligne de

compte. Sur la base d'une première analyse sommaire, nous devons pour l'instant constater que le centre de calcul de la Confédération applique des normes de sécurité plus élevées que le centre de calcul externe. Lors de l'évaluation, la priorité doit être donnée à la solution la plus sûre. Le futur centre de calcul de la Confédération devrait être installé dans un abri protégé. Il s'agit là d'une autre condition dont il faut tenir compte. D'autre part, il n'est pas très opportun de louer de la puissance de calcul auprès d'une société externe pour une durée relativement courte, étant donné que les prix de location ne sont pas négligeables et que les investissements devraient être immédiatement amortis. En l'état actuel de nos connaissances, la préférence doit être donnée à la mise sur pied d'un centre de calcul de secours au sein d'un centre de calcul existant de l'administration fédérale, puisque dans ce cas on peut sans problème investir en matériel et en logiciel que l'on transférera à une date ultérieure dans un abri. Selon nos informations, une telle solution présenterait en outre l'avantage d'être moins chère.
En principe, il faut toujours éviter de traiter des données sensibles sur des systèmes dispersés pour une période de transition s'il n'est pas possible de garantir une dissociation totale et effective de ces données personnelles. Les citoyens sont tenus selon les dispositions légales en vigueur dans l'administration de mettre à disposition entre autres des données sensibles. Il incombe donc également aux organes fédéraux de veiller à ce que ces données soient traitées selon les critères de qualité exigés.

8.6. Procédés d'anonymisation dans le cadre des statistiques médicales des établissements hospitaliers

Dans notre dernier rapport d'activité (p. 158), nous avions mentionné les progrès qui à notre avis avaient été faits au niveau de la protection des données dans le domaine des statistiques médicales des établissements hospitaliers entre avril 1996 et avril 1997. Les incertitudes émises quant au procédé utilisé pour rendre anonymes les données ont entre-temps pu être éliminées en grande partie. Nous décrirons ci-dessous le procédé – généralisable – qui permet une identification des réhospitalisations sans pour autant trahir l'anonymat du patient.

Dans le cadre des statistiques médicales des hôpitaux, il y a lieu de résoudre une contradiction qui existe entre les exigences de la statistique et celles de la protection des données. Pour expliquer ce problème à première vue insoluble, prenons un exemple qui illustre bien les deux types d'exigence: si Monsieur X est hospitalisé en août 1998 à l'hôpital de district A, puis en novembre 1998 à l'hôpital universitaire B, il doit être visible au niveau des statistiques qu'il s'agit les deux fois de la même personne. Par contre, la statistique n'a pas besoin de savoir quelle est la personne qui a été hospitalisée, en d'autres mots elle ne doit pas connaître l'identité de Monsieur X. Dans la terminologie des statisticiens on dira que l'individualisation est nécessaire, l'identification par contre n'est ni utile, ni souhaitable.
L'élaboration des statistiques susmentionnées conformément au concept de détail du printemps 1996 présentait deux points faibles d'importance pour la protection des données, étant donné que l'individualisation (pour retrouver les réhospitalisations) devait être faite en utilisant des variables socio-démographiques telles que le prénom, la date de naissance, le sexe et le numéro postal d'acheminement. Ce procédé s'est cependant avéré être plutôt imprécis et donc peu apte à une individualisation. Il aurait en outre exigé que les caractéristiques mentionnées soient saisies avec un niveau de détail très fin, ce qui aurait permis, à partir des données

en provenance de banques de données centralisées, remonter aux personnes concernées. L'application des concepts existants depuis le printemps 1997 (concept de détail définitif et concept de protection des données) devrait permettre de résoudre les deux problèmes. La modification la plus importante est un procédé basé sur une méthode cryptographique permettant de générer ce qu'on appelle un code de liaison anonyme. Nous présentons ci-dessous les deux caractéristiques principales de ce procédé. Il s'agit en l'occurrence de sélectionner une variable identifiante *ID* et d'y appliquer une fonction *h* qui, à partir de *ID,* génère un code haché *H* à partir duquel il n'est plus possible, par calcul, de retrouver *ID*. Pour assurer l'efficacité de l'opération, il est primordial que cette étape soit exécutée au sein de l'hôpital et que *ID* soit – bien évidemment – immédiatement supprimé une fois que *h* a été appliqué.

Sélection des informations identifiantes ID

Le point de départ est la sélection de certaines informations identifiant une personne hospitalisée *(ID)*, informations qui doivent satisfaire à plusieurs exigences. Elles doivent dépendre uniquement de la personne concernée. Elles doivent subir un minimum de modifications pour la même personne au cours du temps et elles ne doivent pas être de nature à subir facilement des erreurs d'orthographe. En d'autres mots, il s'agit de minimiser la probabilité que l'on attribue deux *ID* distinctes à une seule et même personne. D'autre part, il faut également que la probabilité que deux personnes distinctes correspondent à la même *ID* soit réduite au minimum. La sélection des indications retenues pour *ID* déboucha après des tests sur une chaîne de caractères alphanumériques de 17 positions, qui se compose des champs de données suivants:

- date de naissance exacte à 8 positions sous la forme JJMMAAAA (ce qui donne environ 365 * 120 = 43'800 possibilités pour des personnes vivantes en partant de l'hypothèse que l'âge maximal se situe à 120 ans),
- sexe, une position (2 possibilités),
- code Soundex du prénom (1 lettre et 3 chiffres, au maximum 25'974 possibilités) ainsi que
- code Soundex du nom de famille (1 lettre et 3 chiffres, au maximum 25'974 possibilités).

Ceci donne finalement un nombre total de combinaisons possibles de $5.9 * 10^{13}$. L'application de l'algorithme Soundex sur les chaînes de caractère alphabétiques sert à uniformiser l'orthographe, ce qui est le but principal de cet algorithme. Pour ce faire, cet algorithme convertit les lettres qui «sonnent» la même chose en codes identiques tout en laissant de côté les caractères «non signifiants» tels que les apostrophes, les traits d'union ou les espaces.

Sélection et application d'une fonction h

La fonction doit être la même pour tous les hôpitaux puisque le même code de liaison doit être généré pour un patient donné partout et en tout temps. Ces exigences imposaient plus ou moins l'utilisation d'une fonction de hachage. Une telle fonction présente une propriété «à sens unique» qui, dans ce contexte, s'avère très précieuse. Cela signifie que le code haché peut être calculé de manière efficace en partant de *ID*, l'inverse par contre n'est pas possible. En d'autres mots, il n'est pas possible pour un code *c* donné, au moyen d'une formule, de retrouver les variables utilisées en entrée. Comme chacun le reconnaît, ces exigences peuvent être remplies aussi bien par des fonctions de hachage avec clé (secrète) qu'au moyen de fonctions de hachage sans clé. Une fonction avec clé n'entrait pas en ligne de

compte car le procédé entier aurait vraisemblablement capoté à cause de cette clé. C'est que cette clé aurait dû être la même pour des centaines d'hôpitaux, pour éviter que l'on génère des codes différents pour une même personne dans divers hôpitaux. La clé aurait néanmoins dû être gardée secrète, ce qui au vu du nombre énorme d'utilisateurs aurait été une illusion dès le début. Le choix a été porté sur une invention américaine, le Secure Hash Algorithm (SHA), qui est déjà utilisé depuis plusieurs années avec succès dans le domaine de l'authentification de messages et qui remplit, ce qui est aujourd'hui bien reconnu, l'exigence de fonctionner à «sens unique». Restait finalement ouverte la question importante au niveau des statistiques, à savoir quelle était la probabilité qu'en partant de variables en entrée distinctes *ID* on aboutisse par l'application de *h* au même code. Il fallait absolument étudier en détail cette probabilité, car une telle production artificielle d'hospitalisations multiples aurait exercé une influence très négative sur la signification des statistiques. Des tests effectués avec une base de données contenant environ 222'000 identifications de patients ont révélé une probabilité de 0.003 (ou 0.3%), ce qui a été désigné par les statisticiens comme acceptable au vu des objectifs poursuivis avec ces statistiques.

8.7. Utilisation licite et illicite de codes CIM-10

Il ne relève pas de la compétence du PFPD de donner son avis sur les limites d'utilisation de la Classification Internationale des Maladies, traumatismes et causes de décès (CIM). De telles questions sont du ressort des services responsables du maintien de cette classification et impliqués dans sa révision. L'utilisation de codes CIM-10 peut cependant constituer une violation du principe de la proportionnalité. Tant que cela concerne des traitements de données exécutés par des organes fédéraux ou par des privés, ceci relève de la compétence du PFPD, ce qui signifie que ce dernier peut demander aux organes concernés de modifier leurs traitements.

Pour distinguer les buts d'utilisation appropriés de la classification internationale des maladies, traumatismes et causes de décès des buts non appropriés, il y a lieu de jeter un regard sur les utilisations qui ont été prévues dans le cadre du développement et de la révision de cette classification. La classification initiale date de 1863; elle avait été développée pour permettre l'établissement de statistiques des causes de décès. Dans le cadre de la sixième révision effectuée en 1948, l'OMS a également inclus les maladies et les traumatismes. Finalement, au 1er janvier 1993, la dixième révision a été mise en vigueur par décision de l'assemblée générale de l'OMS. Toutes les révisions entreprises poursuivaient un but : permettre une utilisation des données saisies à des fins de statistiques épidémiologiques. Ceci ressort d'ailleurs du nom de la classification.
Au niveau suisse, cette classification qui comporte environ 13'000 positions a commencé à revêtir une importance nationale lors de l'introduction des statistiques hospitalières, obligatoires pour tous les établissements hospitaliers depuis le 1er janvier 1998. Un concept d'anonymisation des données existe pour ces statistiques depuis le printemps 1997, dont l'application effective permet de dissiper les objections relatives à la protection des données. Il est ainsi possible d'accepter l'utilisation des codes CIM-10 du point de vue de la protection des données, étant donné que d'une part l'on ne peut pas mettre en doute leur aptitude à être utilisés à des fins statistiques et que d'autre part l'anonymisation des données est déjà effectuée à l'échelon de l'hôpital.

Simultanément à l'introduction des statistiques précitées, un grand nombre de nouvelles conventions entre assuranceurs-maladie et établissements hospitaliers sont entrées en vigueur au 1er janvier 1998. Ce qui du point de vue de la protection des données pose problème dans ces accords est que les assureurs se font promettre par les établissements hospitaliers la communication systématique des codes CIM-10. Malgré l'impact important sur la protection des données des flux de données ainsi prévus, le PFPD n'a pas été consulté lors de l'élaboration de ces contrats. De telles communications systématiques de diagnostics très précis dépasse pourtant largement le cadre des flux d'informations prévus par la LAMal, sans compter que cette classification n'est même pas appropriée pour les objectifs non statistiques des assureurs-maladie. Les recherches effectuées jusqu'ici renforcent les présomptions suivantes. Tout d'abord les assureurs ont trouvé très tentant de profiter de l'occasion: suite à l'introduction de la statistique médicale des établissements hospitaliers, un énorme volume de données «était de toute façon déjà saisi » dans les hôpitaux. D'autre part, on était bien conscient du fait que le PFPD considéreraient d'un oeil critique une modification de telle envergure. Dans ce sens, la Conférence nationale des délégués à la protection des données a adopté le 4 novembre 1997 une résolution (voir annexe page 229) s'opposant à ces flux prévus de données. Ces derniers violent non seulement la LAMal, mais également le principe de la proportionnalité, puisque la classification CIM-10 n'est ni nécessaire, ni appropriée pour les buts recherchés. Le problème principal est que l'on mélange des traitements de données qui en fait sont prévus pour des finalités divergentes. On a d'un côté les assureurs qui doivent vérifier les factures et traiter pour cela des données concernant des assurés, donc des patients. Ils sont autorisés pour cela à demander, dans des cas d'espèce, des diagnostics précis, mais certainement pas à les recevoir de manière systématique. La classification par contre n'est pas du tout appropriée pour effectuer ce genre de vérification. D'un côté, les assureurs veulent et doivent conformément au concept de la LAMal développer de nouveaux «produits», en déterminant par exemple les prestataires les meilleurs marchés parmi ceux de bonne qualité et passer avec eux des accords de facturation forfaitaire par cas. Il est évident que pour être en mesure de concevoir de tels contrats, il faut d'abord dépouiller une certain volume de chiffres. Par contre, il semble également clair – et c'est là l'aspect central du point de vue de la protection des données – que de telles analyses ne doivent pas être faites sur la base de données de patients ou d'assurés. Une solution satisfaisante ne peut être trouvée que si l'on dissocie clairement ces deux objectifs. Ce n'est qu'à ce moment qu'il sera possible de déterminer les informations appropriées et nécessaires pour atteindre ces objectifs. Nous somme en contact avec les assureurs pour trouver une solution tenant compte de la séparation susmentionnée.

9. Droit d'accès

9.1. Restriction du droit d'accès

Le Préposé fédéral à la protection des données a été appelé à examiner si l'article 35 LPD pouvait être interprété comme restreignant le droit d'accès de la personne concernée selon l'article 9, 1er alinéa, lettre a LPD.

La situation de départ pour nos recherches concernant la restriction du droit d'accès fut la requête qu'une femme avait adressée à une association qui se déclarait être «religieuse». Cette association défendait le point de vue selon lequel le secret de la confession d'un collaborateur faisait obstacle au droit d'accès.
L'article 8 LPD donne à toute personne le droit de demander à un maître de fichier s'il traite des données la concernant. Selon l'article 9, 1er alinéa, lettre a LPD, ce droit d'accès peut être refusé, restreint ou différé si une loi au sens formel le prévoit. Dans ce cas, c'est l'article 35 LPD qui fut pris en considération. Ce dernier punit quiconque révèle intentionnellement d'une manière illicite des données personnelles secrètes sensibles ou des profils de la personnalité portés à sa connaissance dans le cadre des activités qu'il exerce pour le compte de la personne soumise à l'obligation de garder le secret ou lors de sa formation chez elle. Nous avons renoncé à éclaircir la question de savoir si le collaborateur de l'association pouvait effectivement invoquer le secret de la confession, étant donné que la réponse n'aurait en rien modifié l'issue. L'article 35 LPD stipule que la «révélation illicite» est un acte punissable. Par «révélation» on entend la communication à des tiers. La communication selon l'article 8 LPD est cependant faite à la personne concernée. Celle-ci n'est pas un tiers. Ceci signifie que l'article 35 LPD n'est pas applicable en l'occurrence. Même si le renseignement était donné à un avocat mandaté par la personne concernée, l'article 35 LPD ne serait pas applicable, car dans ce cas le renseignement serait bien donné à un tiers, mais il ne s'agirait pas d'une communication illicite à un tiers étant donné que l'avocat aurait été autorisé par la personne concernée à accepter le renseignement.
Un autre argument avancé par l'association était que l'intérêt prépondérant du confesseur d'observer le secret allait à l'encontre du droit d'accès de la personne concernée. En principe, des informations recueillies par le confesseur sur les déclarations de la personne concernée peuvent aussi contenir des indications sur le confesseur lui-même et devenir ainsi des données personnelles de ce dernier. Selon l'article 9, 1er alinéa, lettre b LPD, le droit d'accès peut être refusé, restreint ou différé si un intérêt prépondérant d'un tiers l'exige. En sa qualité de membre d'une association religieuse ou comme collaborateur de cette dernière, le confesseur ne peut pas être considéré comme un tiers dans ce sens, car le traitement des données le concernant est effectué par le maître du fichier.
En outre, la LPD protège la personnalité du confesseur contre un abus de la part de la personne concernée.

9.2. Exclusion du droit d'accès pour des données personnelles communiquées à l'étranger avant l'entrée en vigueur de la LPD

Nous avons été chargés de clarifier si le droit d'accès était exclu pour des données personnelles envoyées à l'étranger avant l'entrée en vigueur de la LPD.

Les faits à la base de la situation à examiner étaient que des données personnelles avaient été envoyées à l'étranger avant l'entrée en vigueur de la LPD et que la personne concernée faisait valoir son droit d'accès sur ces données. La LPD n'est pas applicable à la collecte et à l'enregistrement de données personnelles antérieurs à la LPD. La même chose est valable pour l'envoi de données à l'étranger. Si au moment de la demande d'accès en revanche, la LPD était déjà en vigueur et que les données personnelles étaient encore disponibles à l'étranger, la conservation ainsi que tout autre traitement des données personnelles à l'étranger peut être considéré

comme un traitement au sens de la LPD. La LPD est alors applicable. L'envoi à l'étranger n'exclut pas l'application de la LPD. Il faut plutôt considérer le traitement de données à l'étranger comme un traitement effectué par des tiers. Conformément à la LPD, le traitement de données personnelles ne peut être confié à un tiers que si le mandant veille à ce que les données ne soient pas traitées au-delà de ce qu'il serait en droit de faire lui-même. Si le maître d'un fichier confie le traitement de données personnelles à un tiers, il garde son obligation de renseigner. Le tiers par contre est tenu de fournir les renseignements s'il refuse de révéler l'identité du maître de fichier ou si ce dernier n'a pas de domicile en Suisse. Il en découle que le droit d'accès est également applicable aux données personnelles qui ont été transférées à l'étranger.

9.3. Droit d'accès après un examen d'admission

On ne peut refuser le droit d'accès en alléguant que les conditions générales l'ont exclu. Les résultats d'examen sont aussi des données personnelles qui doivent être communiquées sur demande à la personne concernée.

Une candidate malheureuse à un poste dans une école privée s'est vu refuser le droit d'accès motif pris qu'en vertu des conditions générales, les candidats n'avaient pas de droit de consultation. Ils pouvaient uniquement, au cours d'un entretien, obtenir des renseignements sur les résultats de l'examen d'admission. La candidate nous a consultés pour savoir si ce procédé était conforme au droit.
La personne qui demande des informations doit avoir accès à toutes les données la concernant figurant dans le fichier. L'information ne peut être refusée que si une loi au sens formel le prévoit ou si les intérêts prépondérants d'un tiers l'exigent, ce qui n'était pas le cas en l'espèce. En outre, un maître privé de fichiers peut refuser ou restreindre la communication des renseignements demandés, voire en différer l'octroi dans la mesure où ses propres intérêts prépondérants l'exigent et à condition qu'il ne communique pas les données personnelles à des tiers. Le droit d'accès ne peut en revanche être refusé en alléguant que les conditions générales l'excluent. D'une part, il s'agit d'un droit inaliénable, imprescriptible et strictement personnel. De l'autre, la personne concernée ne peut être protégée contre elle-même. Il n'existe donc pas de devoir de discrétion à propos de données qui portent sur la personne concernée elle-même. L'institution privée d'enseignement a par la suite modifié ses conditions générales et garantit désormais le droit d'accès.

10. Divers

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

Au début de 1997, nous avons recommandé à une entreprise de cesser la production et la diffusion d'un CD-ROM contenant des données relatives aux détenteurs de véhicules à moteur (cf. 4ème Rapport d'activités, p. 130 ss). Cette recommandation a été rejetée. Nous avons donc porté l'affaire devant la Commission fédérale de la protection des données. Cette dernière, dans sa décision du 18 mars 1998, s'est ralliée à nos conclusions et a confirmé notre recommandation du 17 janvier 1997.

En février 1997, l'avocat de l'entreprise concernée a rejeté notre recommandation demandant de cesser la production et la diffusion de CD-ROM. En revanche, à l'occasion d'un entretien avec l'Association des services des automobiles (ASA) daté de début février 1997, les responsables de l'entreprise en question ont assuré qu'ils ne reprendraient plus la production et la diffusion du CD-ROM. En mars 1997, leur avocat a écrit à tous les Services des automobiles et leur a donné l'assurance que le traitement des données relatives aux détenteurs de véhicules à moteur serait poursuivi en conformité avec la décision éventuelle de la Commission fédérale de la protection des données. Nous avons ensuite porté l'affaire devant ladite commission. Nous avons entre autres requis des mesures provisionnelles en vue de l'arrêt de la production et de la diffusion du CD-ROM en question jusqu'à la décision de la Commission fédérale de la protection des données. Nous avons retiré notre requête suite à la promesse de l'entreprise de surseoir aux dites production et diffusion jusqu'à décision connue. Or l'entreprise n'a respecté qu'une partie de ses engagements, raison pour laquelle nous avons à nouveau menacé de demander la mise en place de mesures provisionnelles.
Le motif de notre recours est essentiellement basé sur la violation des principes suivants: licéité de la collecte de données, proportionnalité, finalité et exactitude. Le défendeur faisait valoir pour l'essentiel que la décision requise par le Préposé fédéral à la protection des données limiterait sa liberté de commerce et d'industrie (LCI). A son avis, il y aurait en outre une inégalité de traitement injustifiée vis-à-vis des fabricants de produits comparables (essentiellement Vidéotexte ainsi qu'une autre entreprise privée). Lors de l'audience publique à laquelle l'entreprise n'a pas assisté malgré sa requête, le préposé s'est exprimé sur la question de la violation de la LCI en ces termes: les maîtres du fichier sont les autorités cantonales et non pas l'entreprise en question. Cette dernière n'est donc pas légitimée à invoquer la LCI. Par ailleurs, la liberté du commerce doit dans tous les cas céder le pas devant les droits protégés de tiers. Les entreprises privées ne peuvent traiter et publier de données relatives aux détenteurs de véhicules à moteur que si le canton a donné expressément son autorisation. L'entreprise en question ne s'est jamais souciée de recueillir une telle autorisation. Pour ce qui est de l'égalité de traitement, le Préposé fédéral à la protection des données a considéré que la situation n'était pas identique à celle des autres prestataires de produits comparables. Pour le reste, l'entreprise ne peut se prévaloir du principe de l'égalité de traitement parce qu'elle a agi de manière illicite. La Commission fédérale de la protection des données, dans sa décision du 18 mars 1998, s'est ralliée à nos conclusions et a confirmé notre recommandation du 17 janvier 1997.

10.2. Vignettes pour vélos et protection des données

On peut se procurer partout en Suisse les vignettes pour vélos sans devoir livrer de données personnelles. Lorsqu'une compagnie d'assurance ne garantit la couverture d'assurance que si les clients lui communiquent leurs données personnelles, il y a infraction à la loi sur la protection des données.

On pouvait lire sur l'emballage de vignettes pour vélos l'indication selon laquelle l'assurance ne couvrait les dommages dans leur totalité que si les clients renvoyaient à l'assurance la carte-réponse jointe. Il fallait mentionner sur cette carte-réponse le nom, l'adresse, le numéro de téléphone, la date de naissance et la profession.

Or les données personnelles qui ne sont pas nécessaires à la conclusion d'un contrat ne doivent être relevées qu'avec le consentement des clients. La personne concernée doit à cette occasion avoir la possibilité de refuser ce consentement sans que cela ait des répercussions négatives sur le contrat. Cela vaut en particulier pour les données qui sont collectées à des fins de marketing et qui n'ont rien à voir avec le contenu du contrat. En l'occurrence, pour la conclusion d'une assurance-vélo, la compagnie d'assurance n'a besoin d'aucune donnée personnelle. La collecte de données sans le consentement du client n'est pas compatible avec la LPD. Par ailleurs, la mention sur l'emballage était à comprendre en ce sens que la couverture d'assurance dépendait de l'envoi de la carte-réponse. Cette méthode est propre à induire le client en erreur (atteinte au principe de transparence).
A la suite de notre intervention, la compagnie d'assurance s'est déclarée prête à détruire les quelque 48'000 cartes-réponses ainsi obtenues en contravention avec la loi.

10.3. Elimination de données personnelles sur puces

De plus en plus de cartes de crédit et de cartes EC contiennent une puce qui permet divers autres traitements. A la fin de la période de validité de la carte, les données contenues dans la puce demeurent encore lisibles même si la carte a été cassée. Un nouvel appareil «déchiqueteur de cartes en plastique» permet une destruction complète des données personnelles.

Diverses entreprises offrent des cartes EC ou des cartes de crédit avec puce intégrée, que l'on peut utiliser par exemple pour téléphoner. Une fois écoulée la période de validité de la carte, il est recommandé de la détruire. Mais casser la carte ne suffit pas à détruire complètement les données personnelles que contient la puce. La lecture de toutes les données enregistrées dans la puce demeure possible et peut éventuellement faire l'objet d'abus. Une entreprise privée vient de mettre au point et de breveter une déchiqueteuse de cartes plastiques qui découpe entièrement la carte en matière synthétique et détruit la puce, permettant de ce fait aussi la destruction de toutes les données.

III. ACTIVITES INTERNATIONALES

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

Le 2 octobre 1997, la Suisse a ratifié la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (voir FF 1997 I 701; voir également 4e rapport d'activités, p. 191). La Convention est entrée en vigueur pour la Suisse le 1er février 1998. Aux côtés de la Suisse, l'Italie et la Hongrie ont également ratifié la Convention en 1997, ce qui porte à 20 le nombre d'Etats parties.

2. Conseil de l'Europe

Lors de sa 602e réunion, le 30 septembre 1997, le Comité des Ministres du Conseil de l'Europe a adopté la Recommandation n° R (97) 18 concernant la protection des données à caractère personnel collectées et traitées à des fins statistiques (voir 4e rapport d'activités, p. 192 et annexe p. 216). Pour sa part, le Groupe de projet sur la protection des données (CJPD) s'est réuni à deux reprises. Il a poursuivi ses travaux en vue de l'adoption d'une recommandation sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance. Cette recommandation régira essentiellement les assurances privées et ne s'appliquera en principe pas aux assurances sociales qui sont couvertes par la Recommandation n° R (86) 1 relative à la protection des données à caractère personnel à des fins de sécurité sociale. Cette approche est regrettable, car du point de vue de la protection des données, les différences entre les assurances sociales et les autres branches d'assurances ne sont pas pertinentes. Cela contribuera aussi à créer une insécurité juridique tant pour l'assuré que pour l'assureur. En outre, le CJPD a examiné en première lecture un projet de lignes directrices sur la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel dans les inforoutes. Dans le cadre de l'utilisation des technologies de l'information (Internet), il est très important d'élaborer une réglementation internationale claire, stable et coordonnée garantissant le respect des droits fondamentaux et en particulier le respect de la vie privée lors du traitement de données personnelles. Un haut niveau de protection des données au plan international est une des conditions indispensables pour permettre le développement d'un environnement informationnel global dans lequel les individus, les consommateurs, les entreprises, les institutions, les collectivités et les autorités puissent communiquer, effectuer des transactions, commercer, échanger des informations, etc. en toute confiance et sécurité. Ce projet de lignes directrices fera vraisemblablement l'objet d'une recommandation du Conseil de l'Europe et pourra être repris dans des codes de conduite. Il doit être une première étape importante et nécessaire en vue d'une réglementation internationale, voire universelle de la protection des données sur Internet. Le projet est rédigé dans un langage accessible à tous. Il énonce les droits et obligations des utilisateurs des inforoutes, ainsi que les devoirs des fournisseurs de service.
Pour sa part, le Groupe de travail n° 15 sur les nouvelles technologies poursuit ses travaux notamment dans le domaine de la surveillance électronique et des cartes à puce. Enfin, un groupe de travail a été chargé d'élaborer un projet de recommandation sur la protection des données dans le domaine des services financiers.

Le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a tenu sa 13e réunion du 10 au 12 décembre 1997. Nous avons représenté la Suisse qui, pour la première fois, participait en tant que partie à la Convention. Le Comité a examiné en première lecture un projet de protocole d'amendement en vue de l'adhésion des communautés européennes à la Convention. Il a en outre décidé d'élaborer des propositions de modifications de la Convention (protocole d'amendement ou protocole additionnel) portant notamment sur la création d'autorités de contrôle indépendantes, le renforcement des compétences du Comité consultatif dans la mise en oeuvre de la Convention et sur les flux transfrontières de données, en particulier à l'égard des Etats tiers.

3. Conférence internationale des commissaires

La XIXe Conférence Internationale des Commissaires à la protection des données s'est déroulée à Bruxelles du 17 au 19 septembre 1997 à l'invitation de la Commission belge de la protection de la vie privée. La Conférence réunissait les commissaires à la protection des données de 24 Etats du monde entier, des experts gouvernementaux, des représentants de la Commission européenne, ainsi que de l'industrie, de l'information, de l'économie, de la science et des services. La Suisse était représentée par le Préposé fédéral suppléant et par le préposé du canton de Zurich. La Conférence était axée autour de deux thèmes principaux, la protection internationale des données et les nouvelles technologies. La Conférence a ainsi abordé le problème des flux transfrontières de données et de ce que l'on entend par protection adéquate des données. A cette occasion, nous avons présenté un contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de données (voir 3e rapport d'activités, p. 215). Ce contrat a été élaboré conjointement par le Conseil de l'Europe, la Commission des Communautés européennes et la Chambre de commerce internationale. Tout en estimant que des clauses contractuelles ne doivent pas se substituer à la nécessité de légiférer dans le domaine de la protection des données, nous avons soutenu que ces clauses constituaient un moyen efficace de pallier l'absence de loi ou de protection adéquate lors de flux transfrontières de données personnelles. Nous avons également recommandé de conclure un tel contrat lors de la communication transfrontière de données vers des Etats ayant une législation équivalente, car cela permet en particulier de préciser les finalités du traitement et les accès légitimes aux données (voir aussi page 185). La Conférence a ensuite débattu de la transposition par les Etats membres de l'Union européenne de la Directive européenne relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, ainsi que de la question de la protection internationale des données dans le domaine de la police. A ce sujet, soulignons en particulier l'appel lancé pour une plus grande harmonisation des normes de protection des données et pour la mise en place d'autorités de contrôle indépendantes. La coopération internationale en matière de police n'est en effet aujourd'hui plus envisageable sans dispositions de protection des données nationales et internationales, notamment pour éviter un développement anarchique de la collaboration et des banques de données qui la sous-tendent. La protection des données plaide également pour une plus grande participation et information des citoyens sur la collecte et la communication transfrontières des données. Les personnes concernées doivent pouvoir avoir connaissance des systèmes et des finalités poursuivies. Les tensions entre la protection des données et la lutte contre la criminalité ne visent pas des objectifs contradictoires; la prise en compte des exigences de la protection des données n'est pas un obstacle à l'efficacité de la lutte contre la criminalité.

En ce qui concerne les nouvelles technologies, retenons en particulier le fait que l'Allemagne a adopté une loi sur les multimédia qui consacre le droit à l'autodétermination en matière d'information dans le domaine des télécommunications. Ce droit est opposable à toute entreprise de télécommunication, ainsi qu'à tout service public ou privé actif dans ce secteur. Cette loi consacre également le droit à l'anonymat lors de l'utilisation d'Internet, l'interdiction des écoutes téléphoniques des téléphones sans fils (Handy) sauf dans le cadre légal et moyennant autorisation. Elle régit le droit de déterminer sous quelle forme et avec

quelles données un utilisateur souhaite figurer dans un annuaire téléphonique, ainsi que la signature digitale.

La Conférence a également abordé la protection des données et les médias, la carte de santé, les écoutes téléphoniques sur les lieux de travail et l'information du public, ainsi que le problème de la protection des données sur Internet, mettant l'accent sur la nécessité de garantir l'anonymat et sur le contrôle par des autorités indépendantes. Il a à nouveau été relevé que les technologies pouvaient offrir des solutions garantissant la protection des données. Plusieurs projets recourant aux technologies de la vie privée sont d'ailleurs en phase de test notamment au Pays-Bas (hôpitaux psychiatriques) et au Canada.

4. OCDE

- Les tentatives de réglementer l'utilisation des procédures de chiffrage

La directive de l'OCDE sur la cryptographie a été adoptée en mai 1997. Cette directive est accompagnée d'un rapport explicatif rédigé par le secrétariat de l'OCDE.

Au cours des trois dernières années, le groupe de travail ad hoc de l'OCDE créé à l'instigation des Etats-Unis a élaboré une directive sur la cryptographie. Durant les travaux, il est apparu que certains pays membres avaient des avis très divergents sur la cryptographie. On pouvait donc distinguer trois différentes tendances. Un groupe mettait l'accent sur la réglementation la plus stricte possible de l'utilisation de la cryptographie. Un autre groupe voulait une politique la plus libérale possible au niveau mondial et un troisième groupe était réservé et observait l'évolution de la question dans les autres pays. La directive adoptée est le résultat de cette situation et tient compte des divers points de vue. Mais, et cela constitue un problème, ces directives sont formulées de manière vague et ne s'expriment pas sur la question centrale du dépôt des clés de chiffrage. Quelques-uns des principes établis par cette directive sont même en contradiction. C'est tout particulièrement le cas des cinquième et sixième principes. Le cinquième principe garantit la protection de la sphère privée et la protection des données. Le sixième principe établit le droit d'accès des autorités étatiques aux informations chiffrées. Dans ces conditions, la directive de l'OCDE – qui n'est pas directement applicable, mais fournit uniquement des consignes d'action pour les Etats membres – est interprétée très différemment par ceux-ci. Il convient de remarquer que même après l'adoption de cette directive qui renferme sciemment des contradictions internes, les Etats-Unis font tout leur possible, par la voie politique, pour que leur politique restrictive en matière de cryptographie se concrétise également dans les autres pays. Ainsi, dès le mois de décembre 1997, un workshop organisé à Paris sur l'initiative des Etats-Unis a réuni des Etats non membres de l'OCDE. Remarquons à ce propos que les pays invités étaient essentiellement ceux qui pratiquent une politique restrictive en matière de cryptographie ou dans lesquels l'utilisation des procédés cryptographiques est tout simplement réservée aux autorités de l'Etat. Durant l'année qui vient, il est prévu que l'OCDE étudie la question des modes d'application de la directive dans les différents Etats membres.
Pour ce qui est de la position du PFPD sur la controverse relative à la cryptographie, se référer au rapport présenté page 187.

- Le groupe d'experts INTERNET

A l'instigation de la Belgique et de la France, l'OCDE a constitué un groupe ad hoc en vue de réglementer les contenus sur INTERNET. Un inventaire des réglementations nationales applicables à INTERNET a été également établi. En octobre 1997, lors de la réunion du groupe ad hoc, les diverses propositions des Etats membres ont été discutées. Il est apparu à cette occasion que la grande majorité de ces pays reconnaissent les problèmes posés par la sécurité et l'application du droit sur INTERNET. Ils ne souhaitent néanmoins pas que ces problèmes soient réglés en priorité par une intervention de l'Etat. Il a donc été établi que le secteur privé doit développer des techniques adaptées aux problèmes qui se posent sur INTERNET (entre autres des mesures de protection pour les mineurs) et que l'OCDE demeure un forum de coordination et d'échange d'informations.
Les discussions qui suivront dans le cadre de l'OCDE sur les problèmes que pose INTERNET rassembleront des représentants du secteur privé, des autorités de protection des données et des organisations de consommateurs.

5. Accord bilatéraux

- Accord avec la France et l'Allemagne sur la collaboration policière transfrontalière

Dans l'accord de Schengen, les Etats de l'Union européenne (UE) ont réglé la collaboration transfrontalière dans les domaines de la migration et de la police. En qualité de non-membre de l'UE, la Suisse s'efforce de mettre en place un «Mini-Schengen» en concluant des accords bilatéraux avec ses voisins. Les accords déjà passés dans le domaine de la migration règlent la protection des données de manière suffisante. Dans le domaine policier par contre, certaines réserves importantes méritent d'être apportées.

La collaboration entre les autorités pénales européennes est réglée par l'accord européen d'entraide judiciaire, des contrats bilatéraux complémentaires ainsi que par la loi fédérale sur l'entraide judiciaire internationale en matière pénale. Selon ces bases légales, des actes d'entraide judiciaire ne sont autorisées que si la gravité du délit est importante, sur demande justifiée et uniquement entre les autorités judiciaires mentionnées. Dans les cas d'urgence particulière, un échange direct d'informations au niveau policier est également admissible. L'accord de Schengen va plus loin et institutionnalise l'entraide judiciaire et administrative directe entre les autorités de police. Il prévoit également que les actes d'entraide judiciaire ne doivent avoir lieu que si la gravité du délit est importante et uniquement par l'intermédiaire des organes centraux de police qui vérifient l'admissibilité et garantissent la coordination. Dans les cas urgents, il prévoit également une collaboration directe entre les organes de police à l'échelon inférieur, ceux-ci devant cependant immédiatement informer les organes centraux et demander leur accord. Ceci est nécessaire parce que l'accord prévoit des délégations réciproques importantes de compétences territoriales dans le domaine de la poursuite pénale (investigation secrète, poursuite transfrontalière). C'est la raison pour laquelle l'accord de Schengen décrit de manière précise tous ces détails.
Dans le cadre de ce que l'on appelle des «Memorandums of Understanding», le Conseil fédéral a délégué des compétences très poussées aux délégations de négociation qui ont pour tâche de négocier par la voie bilatérale des accords avec

nos voisins, accords qui devraient permettre d'intégrer la Suisse dans l'architecture de sécurité de l'Europe. A ce propos, on nous a également demandé notre avis concernant le point de vue de la protection des données. Nous avons constaté qu'il n'y avait pas encore beaucoup d'idées concrètes en ce qui concerne la protection des données, que d'un autre côté on considérait l'accord de Schengen très détaillé en comparaison (avec protection des données sectorielle explicite) comme étant trop restrictif dans certains domaines. Au vu de cette situation, nous avons décidé de procéder à une analyse précise des traitements de données actuels dans le cadre de la collaboration policière dans la zone frontière, d'élaborer des dispositions standard en matière de droit sur la protection des données pour les contrats prévus et d'expliquer aux délégations quels traitements de données prévus seraient à notre avis illicites. Quant à la question relevant de l'état de droit, de savoir dans quelle mesure la collaboration policière dans le cadre des accords bilatéraux pourrait et devrait dépasser ce qui a été prévu dans l'accord de Schengen, nous n'avons pas émis d'opinion par défaut de compétence.

Par la suite, nous avons assisté aux traitements de données effectués par le corps des gardes-frontière à Genève et à Neuhausen. Nous avons également pu jeter un œil sur les traitements de données d'une autorité de police cantonale proche de la frontière. A cette occasion nous avons présenté aux participants un catalogue des problèmes de protection des données liés aux traitements de données transfrontalières, catalogue que nous avons également expliqué aux délégations de négociations. Il nous semble important qu'une instance de contrôle policière centrale soit responsable de la protection des données et puisse l'assurer. Il faut quelqu'un qui décide d'après des critères précis quelles données policières peuvent être communiquées à une autorité de police étrangère, dans quelles circonstances, dans quels buts et avec quelles charges. Ainsi, les données recueillies dans le cadre d'une investigation secrète concernant des citoyens n'ayant rien à se reprocher (tiers non impliqués) doivent être immédiatement détruites et ne peuvent pas être emportées à l'étranger par les organes de police étrangers qui enquêtent en Suisse. Le problème se pose de manière encore plus accentuée dans le cas où des données non vérifiées concernant des réfugiés sont communiquées par la police aux organes de police à l'étranger qui sont reliés entre eux par l'intermédiaire d'Interpol. En général, il y a lieu de définir clairement ce qui se passe avec des données non vérifiées à l'étranger et quelles exigences (sévères) doivent être remplies pour que de telles données puissent le cas échéant être communiquées à d'autres autorités. Des organes de police étrangers ne sont en outre pas autorisés à accéder par procédure d'appel aux fichiers de données personnelles en Suisse. L'entraide administrative – par exemple aux postes frontière très fréquentés – doit être réglée différemment.

Même si nous ne sommes pas représentés en permanence dans les délégations de négociations, nous espérons que ces questions importantes, qui sont bien entendu également dans l'intérêt de la police, trouveront une bonne solution en ce qui concerne la protection des données. Nous considérons nos propositions pour des dispositions sectorielles de protection des données comme une contribution importante permettant d'atteindre cet objectif.

6. Rapports délicats entre l'asile et l'entraide judiciaire internationale

Les traitements de données effectués à l'occasion d'une demande d'entraide judiciaire internationale ont mené à de nombreuses interpellations. Nos recherches auprès de l'Office fédéral des réfugiés n'ont révélé aucun traitement de données illicite. Par contre, nous avons demandé que l'échange de données avec l'Office fédéral de la police soit décrit en détail dans un règlement de traitement.

La fuite spectaculaire d'un présumé terroriste d'une prison de haute sécurité à l'étranger, sa demande d'asile en Suisse, la demande d'entraide judiciaire subséquente du gouvernement étranger et l'arrestation qui suivit ont eu un grand écho dans tous les médias de Suisse et ont également mené à des interpellations sur le plan politique. A cette occasion, on nous a à plusieurs reprises posé la question si certains événements ne laissaient pas présumer que des transmissions illicites de données avaient eu lieu depuis la Suisse vers les autorités de justice militaire de l'état étranger en question. Il s'agit d'un Etat auquel on reproche régulièrement de pratiquer la torture.
Selon la loi sur la protection des données, nous ne sommes pas autorisés à vérifier le trafic qui a eu lieu dans le cadre d'une procédure d'entraide judiciaire entre les autorités d'entraide judiciaire suisses et étrangères. Ceci relève de la compétence d'autres autorités et en dernière instance du Tribunal fédéral, qui dans ce cas tient également compte de l'interdiction au niveau international de pratiquer la torture. Nous pouvons par contre vérifier si des organes autres que les autorités d'entraide judiciaire ont sans base légale communiqué des données sensibles, confidentielles – par exemple sur la procédure d'asile – à des autorités suisses ou étrangères. D'autre part, nous pouvons vérifier si l'autorité d'entraide judiciaire a transmis les données personnelles qu'elle a reçu par exemple sur la procédure d'asile à une autorité étrangère sans qu'un lien existe avec une procédure d'entraide judiciaire ou sans avoir pris contact avec le maître de fichiers pour peser préalablement les intérêts de cette communication.
Dans le cadre de notre enquête, l'Office fédéral des réfugiés nous a bien renseigné sur les traitements de données qu'il a effectué dans le cas précis. Nous n'avons pas pu déceler de violations du droit sur la protection des données. Nous avons par contre dû critiquer l'absence d'un règlement de traitement pour les communications de données délicates entre l'Office fédéral des réfugiés et l'Office fédéral de la police. Un tel règlement devrait décrire de manière plus précise les dispositions applicables en la matière de la loi sur l'asile complètement révisée et devrait être élaboré sans tarder.

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

Le groupe de travail, présidé par le préposé à la protection des données de Berlin, a pour objectif d'améliorer la protection des données dans le domaine des télécommunications et des médias. La discussion ainsi que l'échange d'expériences dans ce domaine sont très précieux pour le PFPD. A la 22ème séance du 27 septembre 1997, on a entre autres abordé les développements du droit des télécommunications. On a débattu de problèmes de protection des données – mais aussi de nouvelles techniques telles que la «Platform for Privacy - P3P» du

consortium WWW – en rapport avec Internet, et on a rédigé une prise de position critique quant aux efforts de réglementation de la cryptographie.

IV. PREPOSE FEDERAL A LA PROTECTION DES DONNEES

1. Quatrième Conférence suisse des commissaires à la protection des données (1997)

La quatrième Conférence suisse des commissaires à la protection des données s'est déroulée au Castelgrande à Bellinzone, le 3 novembre 1997. Elle était organisée par le préposé à la protection des données du canton du Tessin. Cette conférence annuelle réunit le Préposé fédéral à la protection des données, les commissaires cantonaux et communaux à la protection des données et les autres responsables cantonaux de la protection des données. Outre le Préposé fédéral, 18 cantons et 2 communes étaient présents.

Les sujets suivants ont été abordés: les registres centralisés et les problèmes de protection des données qu'ils soulèvent, Internet (sécurité et surveillance des collaborateurs), protection des données dans le secteur de la police, les droits de contrôle du préposé à la protection des données, la communication électronique des données dans le secteur de la santé, la protection des données dans le domaine des assurances sociales.
La Conférence a également adopté une résolution relative à la communication aux assureurs des codes de diagnostics CIM-10 (voir annexe p. 229). La Conférence exige en particulier que d'une part, le flux soit limité aux données nécessaires et propres à atteindre le but recherché et, d'autre part, que l'on renonce à l'introduction prévue des codes CIM-10 pour le contrôle des factures. Afin de pouvoir assurer le secret médical, les contrôles des coûts et d'économicité ne doivent pas être effectués par assuré mais par cas. De la sorte, les services administratifs des assureurs ne seront pas saturés par des transferts de données inutiles, ni le secret médical mis en question. Il pourrait même s'agir d'une contribution active à la limitation des coûts de la santé (voir aussi supra, p. 195 ss).
Pour sa part le groupe de travail des préposés cantonaux à la protection des données s'est réuni à quatre reprises et a abordé en particulier des questions dans les domaines de la santé, de la statistique, de l'emploi, de la police, du droit des étrangers et de la circulation routière (publication des numéros d'immatriculation des véhicules). Il s'est également penché sur ses méthodes de travail et a décidé d'introduire, à titre d'essai, une présidence annuelle et de créer des sous-groupes. Nous avons pris part régulièrement aux travaux de ce groupe de travail.

2. Les publications du PFPD

- Information sur les études de marché et sondages d'opinion à des fins privées
- Information sur les formulaires d'inscription relatifs à la location d'un appartement
- Information sur les répercussions de la loi sur l'égalité

3. Statistique des activités du PFPD

Période du 1er avril 1997 au 31 mars 1998

Nombre de prises de position

Nombre de prises de position

Renseignements par telephone

Renseignements par téléphone
Selon la provenance des appels

Renseignements par téléphone
Par matière

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

Préposé fédéral à la protection des données : Guntern Odilo, dr en droit

Suppléant : Walter Jean-Philippe, dr en droit

Secrétariat :

Chef : Walter Jean-Philippe, dr en droit

Suppléante : Grand Carmen, lic. en droit

Délégué Presse et Information : Tsiraktsopulos Kosmas, lic. en droit

Service juridique : 9 Personen

Service informatique : 4 Personen

Chancellerie : 3 Personen

V. ANNEXES

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

RECOMMANDATION No R (97) 18

DU COMITÉ DES MINISTRES AUX ÉTATS MEMBRES

CONCERNANT LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

COLLECTÉES ET TRAITÉES À DES FINS STATISTIQUES

(adoptée par le Comité des Ministres le 30 septembre 1997,
lors de la 602e réunion des Délégués des Ministres)

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

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

Conscient des besoins, aussi bien dans le secteur public que dans le secteur privé, de statistiques fiables pour l'analyse et la compréhension de la structure et de l'évolution de la société contemporaine, et pour la définition des politiques et des stratégies pour les mesures à prendre dans pratiquement tous les domaines de la vie quotidienne;

Reconnaissant que la production de statistiques fiables dépend largement de la collecte des informations aussi complètes que possible, et du traitement de telles informations par des moyens informatiques toujours plus performants;

Conscient du fait que de telles informations peuvent concerner des personnes physiques identifiées ou identifiables («données à caractère personnel»);
Conscient de la nécessité de développer des techniques permettant de garantir l'anonymat des personnes concernées;

Considérant les préoccupations de la communauté internationale des statisticiens au sujet de la protection des données à caractère personnel, ainsi que le développement des recommandations internationales en matière d'éthique professionnelle des statisticiens;

Considérant également les principes fondamentaux de la statistique officielle adoptés par la communauté internationale dans le cadre de l'Organisation des Nations Unies;

Constatant le développement progressif de normes juridiques nationales et supranationales tant en matière d'activités statistiques que dans le domaine de la protection des données à caractère personnel;

Rappelant à cet égard les principes généraux relatifs à la protection des données de la Convention pour la protection des personnes à l'égard du traitement automatisé des

données à caractère personnel (Strasbourg 1981, Série des traités européens no 108);

Rappelant également les dérogations admises en faveur des activités statistiques dans la convention à l'égard de l'exercice, par les personnes concernées, de certains droits énoncés dans la convention;

Constatant que des dérogations en ce sens sont également prévues par plusieurs Etats membres dans les législations existantes ou en cours d'élaboration en matière de protection des données;

Considérant qu'il convient de trouver un équilibre entre la nécessité de la production des statistiques d'une part, et l'indispensable protection de la personne d'autre part, notamment lorsque des traitements automatisés de données sont utilisés;

Conscient de la nécessité d'établir des procédures appropriées visant à concilier les intérêts des différentes parties concernées;

Conscient du fait que le progrès accompli dans les méthodes statistiques et les développements intervenus dans la technologie de l'information depuis 1983 nécessitent la révision de plusieurs dispositions de la Recommandation no R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques,

Recommande aux gouvernements des Etats membres:

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

- d'assurer une large diffusion des principes contenus dans l'annexe à la présente recommandation parmi les personnes, autorités publiques et organismes qui collectent et traitent des données à caractère personnel à des fins statistiques, dans les secteurs tant public que privé, ainsi que parmi les instances compétentes en matière de protection des données;

- d'encourager ces personnes, autorités publiques et organismes à introduire, s'ils ne l'ont pas encore fait, des codes d'éthique inspirés par l'annexe à la présente recommandation;

Décide que la présente recommandation remplace la Recommandation no R (83) 10 relative à la protection des données à caractère personnel utilisées à des fins de recherche scientifique et de statistiques, dans la mesure où cette recommandation s'applique à la collecte et au traitement automatisé de données à caractère personnel à des fins statistiques.

Annexe à la Recommandation no R (97) 18

1. Définitions

Aux fins de la présente recommandation:

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

- l'expression «données d'identification» recouvre les données à caractère personnel qui permettent l'identification directe de la personne concernée et qui sont nécessaires à la collecte, au contrôle et à l'appariement des données, mais qui ne sont pas utilisées par la suite pour établir des résultats statistiques.

- l'expression «données sensibles» signifie les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé, à la vie sexuelle ou concernant des condamnations pénales, ainsi que les autres données définies comme sensibles par le droit interne.

- l'expression «traitement» recouvre toute opération ou ensemble d'opérations effectués partiellement ou totalement à l'aide de procédés automatisés, et appliqués à des données à caractère personnel, telles que l'enregistrement, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, l'appariement ou l'interconnexion, ainsi que l'effacement ou la destruction.

Le terme «communication» signifie l'acte de rendre accessibles à des tiers des données à caractère personnel, quels que soient les moyens ou les supports utilisés.

- l'expression «à des fins statistiques» se réfère à toutes opérations de collecte et de traitement de données à caractère personnel nécessaires aux enquêtes statistiques ou à la production de résultats statistiques. De telles opérations excluent toute utilisation de l'information obtenue pour des décisions ou des mesures relatives à une personne déterminée.

- l'expression «résultats statistiques» désigne une information obtenue par le traitement de données à caractère personnel en vue de caractériser un phénomène collectif dans une population considérée.

- l'expression «responsable du traitement» s'entend de la personne physique ou morale, de l'autorité publique ou de tout autre organisme qui, seul ou avec la collaboration d'autres, détermine les finalités et les moyens – notamment l'organisation – de la collecte et du traitement des données à caractère personnel.

2. *Champ d'application*

2.1. La présente recommandation s'applique à la collecte et au traitement automatisé de données à caractère personnel à des fins statistiques.

Elle s'applique aussi aux résultats statistiques, dans la mesure où ceux-ci permettraient l'identification des personnes concernées.

2.2. Les Etats membres sont encouragés à étendre l'application de la présente recommandation aux traitements non automatisés des données à caractère personnel à des fins statistiques.

2.3. Un traitement de données à caractère personnel ne doit pas être effectué de manière non automatisée dans le but d'échapper aux dispositions de la présente recommandation.

2.4. Les Etats membres peuvent étendre l'application des principes énoncés dans la présente recommandation également à la collecte et au traitement de données relatives aux groupements de personnes, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique.

3. *Respect de la vie privée*

3.1. Le respect des droits et des libertés fondamentales, et notamment du droit à la vie privée, doit être garanti lors de la collecte et du traitement des données à caractère personnel à des fins statistiques, ainsi que

a. lors de la conservation de ces données pour une utilisation future;

b. lors de la diffusion de résultats statistiques; et

c. lors de la modification éventuelle des données à caractère personnel alors que cette modification s'impose pour améliorer la représentativité des résultats statistiques ou pour des raisons de confidentialité.

3.2. Le droit ou la pratique internes doivent soumettre au secret professionnel les personnes qui, à l'occasion d'une activité statistique, ont connaissance de données à caractère personnel.

3.3. Les données à caractère personnel collectées et traitées à des fins statistiques doivent être rendues anonymes dès qu'elles ne sont plus nécessaires sous une forme identifiable.

4. *Conditions générales régissant la collecte et le traitement à des fins statistiques*

Finalité

4.1. Les données à caractère personnel collectées et traitées à des fins statistiques doivent servir uniquement à ces fins. Elles ne doivent pas être utilisées pour prendre une décision ou mesure relative à la personne concernée ou pour

compléter ou corriger des fichiers dont les données à caractère personnel sont traitées pour des finalités non statistiques.

4.2. Le traitement à des fins statistiques de données à caractère personnel collectées à des fins non statistiques n'est pas incompatible avec la/les finalité(s) pour lesquelles les données ont été initialement collectées, dans la mesure où des garanties appropriées sont prévues notamment pour empêcher l'utilisation des données à l'appui de décisions ou de mesures relatives à la personne concernée.

Licéité

4.3. Les données à caractère personnel peuvent être collectées et traitées à des fins statistiques:

a. si la loi le prévoit; ou

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

i. si la personne concernée ou son représentant légal y a consenti conformément au principe 6; ou
ii. si la personne a été informée de la collecte ou du traitement de ses données et ne s'y est pas opposée et pour autant que le traitement ne porte pas sur des données sensibles; ou
iii. si les circonstances de la collecte et l'objectif de l'enquête sont de nature à permettre qu'une personne puisse répondre au nom et en place d'autres personnes conformément au principe 6 et pour autant qu'il n'existe manifestement aucun risque d'atteinte à la vie privée de ces personnes, et notamment que le traitement ne porte pas sur des données sensibles.

4.4. Afin d'éviter que les mêmes données ne soient collectées une nouvelle fois, les données à caractère personnel collectées à des fins non statistiques peuvent également être traitées à des fins statistiques si cela est nécessaire:

a. à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique; ou

b. à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement à condition que ne prévalent pas les droits et les libertés fondamentales de la personne concernée.

Dans les mêmes conditions, les données collectées pour une finalité statistique peuvent également être traitées pour d'autres finalités statistiques.

4.5. Les données à caractère personnel ne peuvent être collectées à titre contraignant en vue d'un traitement à des fins statistiques que si le droit interne l'exige.

4.6. Des données à caractère personnel ou des ensembles de données à caractère personnel peuvent être appariés ou mis en relation à des fins statistiques si le

droit interne aménage des garanties appropriées pour empêcher leur traitement et leur communication à des fins non statistiques.

Proportionnalité

4.7. La collecte et le traitement de données à caractère personnel doivent être limités aux seules données nécessaires aux finalités statistiques poursuivies. En particulier, les données d'identification ne doivent être collectées et traitées que si cela est nécessaire.

Données sensibles

4.8. Si des données sensibles sont traitées à des fins statistiques, ces données devraient être collectées sans que les personnes concernées soient identifiables.

Si l'objectif légitime et spécifique d'un traitement de données sensibles à des fins statistiques rend nécessaire le fait que les personnes concernées soient identifiées, le droit interne doit prévoir des garanties appropriées, y compris des mesures spécifiques pour séparer les données d'identification, dès la collecte, sauf si cela est manifestement déraisonnable ou infaisable.

5. *L'information des personnes*

Collecte primaire

5.1. Lorsque, à des fins statistiques, des données à caractère personnel sont collectées, les personnes interrogées doivent être informées des éléments suivants:

a. le caractère obligatoire ou facultatif des réponses et le fondement juridique éventuel de la collecte;

b. la ou les finalités de la collecte et du traitement;

c. le nom et le statut de la personne ou de l'organisme responsable de la collecte et/ou du traitement;

d. le fait que ces données seront tenues confidentielles et utilisées uniquement à des fins statistiques;

e. la possibilité d'obtenir sur demande d'autres informations.

A leur demande et/ou selon des modalités définies par le droit interne, les personnes concernées doivent également être informées:

f. en cas d'enquête facultative, sur les modalités de refus ou de retrait du consentement et, en cas d'enquête obligatoire, sur les sanctions éventuelles;

g. le cas échéant, sur les conditions d'exercice du droit d'accès et de rectification;

h. sur les catégories de personnes ou d'organismes auxquels les données à caractère personnel pourront être communiquées;

i. sur les garanties pour assurer la confidentialité et la protection des données à caractère personnel;

j. sur les catégories de données collectées et traitées.

5.2. Lorsqu'elles ne sont pas directement interrogées, les personnes concernées doivent être informées de l'existence de la collecte, sauf si cela est manifestement déraisonnable ou infaisable. Elles doivent avoir la possibilité de s'informer de manière appropriée des éléments mentionnés au principe 5.1.

5.3. Les personnes interrogées, qu'elles soient concernées ou non, doivent être informées au plus tard au moment de la collecte des données. Les modalités et l'étendue de l'information doivent être appropriées et adaptées aux circonstances.

Lorsque cela est nécessaire pour atteindre l'objectif légitime de l'enquête, en raison de son objet et de sa nature, la fourniture de l'information ou d'une partie de l'information peut être différée. Celle-ci devra alors être fournie dès que cette nécessité n'existe plus, sauf si c'est manifestement déraisonnable ou infaisable. Dans de telles circonstances, lorsque les données ont été collectées auprès de la personne concernée, l'information devrait lui être fournie à un stade ultérieur.

Collecte secondaire

5.4. Le traitement ou la communication à des fins statistiques des données à caractère personnel collectées à des fins non statistiques fait l'objet d'une publicité appropriée. Les personnes concernées doivent avoir la possibilité de s'informer de manière appropriée des éléments mentionnés au principe 5.1. à moins que:

a. la fourniture de l'information ne se révèle impossible ou implique des efforts disproportionnés; ou que

b. le traitement ou la communication des données à des fins statistiques ne soit expressément prévu par le droit interne.

Dans les cas visés aux lettres a et b, des garanties appropriées doivent être prévues.

Incapables légaux

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

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

6. *Consentement*

6.1. Lorsque le consentement de la personne concernée est requis, celui-ci doit être libre, éclairé et indubitable.

La personne concernée doit avoir la possibilité soit de retirer son consentement pour une enquête unique, avant que les données d'identification ne soient séparées des autres données collectées, soit d'interrompre à tout moment et sans effet rétroactif sa coopération à une enquête échelonnée dans le temps.

6.2. S'il est requis pour la collecte ou le traitement de données sensibles, le consentement donné par la personne doit être explicite, libre et éclairé. L'objectif légitime de l'enquête ne peut être considéré comme dispensant de recueillir un tel consentement que si un motif d'intérêt public important justifie cette dérogation.

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

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

6.4. Le refus de répondre ne doit pas faire l'objet de sanctions, sauf si celles-ci sont prévues par le droit interne.

7. *Droits d'accès et de rectification*

7.1. Toute personne peut obtenir la communication des données à caractère personnel la concernant détenues par le responsable du traitement et en obtenir, le cas échéant, la rectification.

7.2. Cependant, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, ce droit peut être restreint conformément au droit interne lorsque les données à caractère personnel sont traitées uniquement à des fins statistiques et qu'existent des mesures spécifiques appropriées pour prévenir toute identification par un tiers, tant à partir des données individuelles qu'à partir des résultats statistiques.

8. *Anonymat*

8.1. Les données à caractère personnel collectées à des fins statistiques seront rendues anonymes dès la fin des opérations de collecte, de contrôle ou d'appariement, sauf:

a. si des données d'identification demeurent nécessaires à des fins statistiques et que les mesures prévues au principe 10.1 ont été prises; ou

b. si la nature même du traitement statistique nécessite de démarrer les autres opérations de traitement avant que les données n'aient été rendues anonymes, et pour autant que les mesures de sauvegarde prévues aux principes 15.1 à 15.3 soient mises en œuvre.

9. *Collecte primaire des données à caractère personnel à des fins statistiques*

9.1. La collecte des données à caractère personnel doit être loyale, notamment en ce qui concerne l'information des personnes et leur liberté de répondre.

9.2. La collecte de données à caractère personnel est effectuée auprès de la personne concernée ou, selon la nature de l'enquête, peut l'être auprès d'un membre de son ménage. La collecte de données à caractère personnel auprès d'une personne autre que la personne concernée elle-même ou d'un membre de son ménage, ainsi que la collecte auprès d'entités juridiques telles que des entreprises ou des collectivités publiques, ne doit être effectuée que si le droit interne le prévoit et aménage des sauvegardes appropriées, ou lorsqu'il n'existe manifestement pas de risque d'atteinte aux droits et aux libertés fondamentales des personnes concernées.

9.3. La collecte à des fins statistiques de données à caractère personnel sans interrogation ne doit ni comprendre de données d'identification ni être mise en relation avec des données d'identification, sauf si le droit interne aménage des sauvegardes appropriées et

a. prévoit la collecte avec des données d'identification, ou

b. permet la mise en relation de données collectées avec des données d'identification en vue de l'établissement d'échantillons.

9.4. Les données concernant les non-répondants qui sont pertinentes au plan ou à l'exécution de l'enquête, et des informations sur les raisons de l'absence d'une réponse, ne peuvent être utilisées que pour assurer la représentativité d'une enquête.

9.5. Lorsque la collecte de données à caractère personnel nécessite le recours à des enquêteurs ou à d'autres personnes qui ont à connaître directement des réponses fournies, une attention particulière doit être portée quant au choix des personnes et au choix de l'organisation et des méthodes d'enquête, afin de garantir le respect de la finalité de l'enquête, la confidentialité des données et la protection de la vie privée.

9.6. Le responsable du traitement doit prendre des mesures appropriées qui permettent à la personne interrogée de s'assurer de la légitimité de la personne qui collecte les données.

10. *Données d'identification*

10.1. Lorsque des données d'identification sont collectées et traitées à des fins statistiques, elles doivent être séparées et conservées séparément des autres données à caractère personnel, sauf si cela est manifestement déraisonnable ou infaisable.

10.2. Les données d'identification peuvent être utilisées pour créer un fichier d'adresses à des fins statistiques si le droit interne le prévoit, si la personne concernée a été informée et ne s'y est pas opposée ou si elles proviennent d'un fichier accessible au public.

11. *Conservation des données*

11.1. A moins qu'elles ne soient rendues anonymes ou que la loi interne ne prévoie leur conservation à des fins d'archivage moyennant des garanties appropriées, les données à caractère personnel collectées et traitées à des fins statistiques doivent être détruites ou effacées lorsqu'elles ne sont plus nécessaires à ces fins.

En particulier, les données d'identification doivent être détruites ou effacées dès qu'elles ne sont plus nécessaires:

a. aux opérations de collecte, de contrôle et d'appariement des données; ou

b. pour assurer la représentativité de l'enquête; ou

c. pour répéter une enquête avec les mêmes personnes.

12. *Communication*

12.1. Les données à caractère personnel collectées à des fins statistiques ne doivent pas être communiquées à des fins non statistiques.

12.2. Des données à caractère personnel qui sont traitées pour une finalité statistique particulière peuvent être communiquées pour d'autres finalités statistiques pour autant que celles-ci soient spécifiées et limitées dans le temps.

12.3. A moins que des sauvegardes pour la communication ne soient prévues par le droit interne, une communication en conformité avec le principe 12.2 devra faire l'objet d'un document écrit matérialisant les droits et devoirs des parties. Lors de la communication des données, le responsable du traitement doit en particulier:

a. stipuler que ce tiers ne peut communiquer lui-même les données en question qu'avec l'accord exprès dudit responsable du traitement;

b. stipuler que ce tiers prend les mesures de sécurité appropriées conformes aux principes 15.1 à 15.3 de la présente recommandation;

c. s'assurer que toute publication des résultats statistiques obtenus par ce tiers est conforme au chapitre 14 de la présente recommandation.

12.4. De surcroît, les données sensibles peuvent être communiquées uniquement si la loi le prévoit ou si la personne concernée ou son représentant légal y a explicitement consenti pour autant que le droit interne ne s'y oppose pas.

13. *Flux transfrontières de données*

13.1. Les principes de la présente recommandation sont applicables à la communication transfrontière de données à caractère personnel à des fins statistiques.

13.2. La communication transfrontière de données à caractère personnel vers un Etat ayant ratifié la Convention no 1081 et disposant d'une législation assurant une protection des données pour le moins équivalente ne devrait pas être soumise à des conditions particulières de protection de la vie privée, des droits et des libertés fondamentales des personnes.

13.3. Il ne devrait pas y avoir de limitation à la communication transfrontière de données à caractère personnel à des fins statistiques vers un Etat n'ayant pas ratifié la Convention no 108 lorsque celui-ci assure un niveau de protection conforme aux principes de ladite convention et de la présente recommandation.

13.4. A moins que le droit interne n'en dispose autrement, la communication transfrontière de données à caractère personnel à des fins statistiques vers un Etat n'assurant pas une protection conforme aux principes de la Convention no 108 et de la présente recommandation ne devrait en règle générale pas intervenir, à moins que:

a. des mesures nécessaires, y compris de nature contractuelle, au respect des principes de la convention et de la présente recommandation n'aient été prises; ou que

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

14. *Résultats statistiques*

14.1. Les résultats statistiques ne doivent être publiés ou rendus accessibles à des tiers que si des mesures sont prises pour s'assurer que les personnes concernées ne sont plus identifiables sur la base de ces résultats, à moins que la diffusion ou la publication ne présente manifestement pas de risque d'atteinte à la vie privée de ces personnes.

15. *Sécurité des données*

15.1. Les responsables de traitements doivent veiller à assurer la confidentialité des données à caractère personnel par des mesures techniques et d'organisation appropriées. Ils prennent en particulier des mesures contre l'accès, la modification, la communication ou toute autre forme de traitement non autorisés.

15.2. Lorsque les données doivent être conservées sous une forme identifiable, il doit être fait usage de ressources organisationnelles et techniques, notamment informatiques, pour prévenir une identification non autorisée de la personne concernée.

15.3. Des mesures doivent être prises pour empêcher que les personnes concernées puissent être réidentifiées et que des données à caractère personnel collectées à des fins statistiques puissent être utilisées à des fins non statistiques.

15.4. Les professionnels, les entreprises et les organismes chargés de l'établissement des statistiques doivent mettre au point des techniques et des procédures permettant d'assurer l'anonymat des personnes concernées.

16. *Codes d'éthique*

16.1. Les professionnels, les entreprises et les organismes chargés de l'établissement de statistiques devraient adopter et rendre publics des codes d'éthique professionnelle conformes à la présente recommandation et assortis d'informations notamment:

a. sur les autres catégories de personnes et d'organismes ayant accès aux données à caractère personnel;

b. sur les mesures de protection, de confidentialité et de sécurité de ces données, ainsi que d'éthique statistique; et

c. sur les responsables du traitement statistique.

17. *Développement technique, coopération et assistance*

Afin d'assurer un large accès aux outils informatiques et aux connaissances techniques appropriées à une protection efficace des données à caractère personnel collectées à des fins statistiques, les instances gouvernementales compétentes devraient collaborer étroitement dans le développement de ces outils et de ces connaissances et mettre sur pied des programmes internationaux de coopération, d'échange d'expériences, de transfert de connaissances et d'assistance technique.

18. *Autorités de surveillance*

Les Etats membres chargent une ou plusieurs autorités indépendantes de veiller au respect de l'application du droit interne mettant en œuvre les principes énoncés dans la présente recommandation.

_____

1. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg,
28 janvier 1981 (Série des traités européens no 108).

2. Directives de l'Organisation internationale du travail

- Les employés ont droit au respect de leur sphère privée sur le lieu de travail.

- Les employés doivent savoir quelles sont les méthodes de surveillance utilisées et connaître l'usage que l'employeur fait des données ainsi recueillies.

- L'employeur doit recourir aussi rarement que possible à des moyens de surveillance ou d'exploration des fichiers, des communications sur réseau ou du courrier électronique. La surveillance électronique permanente est interdite.

- Les employés doivent être associés aux décisions concernant l'opportunité et la manière d'employer des moyens de surveillance ou d'exploration.

- Des données ne peuvent être recueillies et utilisées qu'à des fins clairement définies et en rapport avec le travail.

- Il ne peut être procédé à des surveillances ou à des explorations sans information préalable des employés que si des indices sérieux permettent de présumer la commission d'actes criminels ou d'autres formes d'abus.

- L'évaluation des prestations des employés ne peut se baser uniquement sur les résultats d'une surveillance.

- Les employés ont le droit de consulter, de contester et d'exiger la rectification des données recueillies à leur sujet par le biais de la surveillance électronique.

- Les enregistrements qui ne sont plus nécessaires au but dans lequel ils ont été réalisés doivent être détruits.

- Les données recueillies lors d'une surveillance et qui permettent une identification individuelle des employés ne peuvent être communiquées à des tiers, à moins qu'une obligation légale existe à cet égard.

- Les employés ou les futurs employés ne peuvent renoncer au droit à la protection de leur sphère privée.

- Tout supérieur qui viole ces principes est passible de mesures disciplinaires ou de licenciement.

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

3. Résolution de la IVème Conférence nationale des Préposés à la protection des données

- La communication aux assureurs des codes de diagnostics CIM-10 viole le secret médical

La Conférence nationale des Préposés à la protection des données partage les craintes des hôpitaux, des médecins et des patients qu'un flux de données croissant à destination des assurances mette en question le secret médical. Ce flux de données génère non seulement un surcroît de travail générateur de dépenses mais est également contraire à l'esprit de la loi sur l'assurance-maladie (LAMal). Une grande masse d'informations circule de plus en plus fréquemment et automatiquement des hôpitaux vers les assureurs, et ce souvent à l'insu des personnes concernées. A cette occasion, les assureurs exigent que les informations concernant les diagnostics soient livrées dans tous les cas et sans condition sous une forme détaillée correspondant aux codes de diagnostics CIM-10 qui englobent plus de 10'000 positions. Il est vrai que la LAMal donne le droit aux assureurs, dans des cas d'espèce, d'exiger des indications détaillées. La communication d'une telle masse d'information n'est par contre pas couverte par la LAMal. Ainsi le secret médical serait contourné, le médecin-conseil ne pouvant plus traiter la masse de données ni empêcher par conséquent le passage direct de données sensibles concernant la santé vers les services administratifs des assureurs. Le flux de données critiqué est en outre excessif et à long terme également dangereux pour les raisons suivantes:

Le code CIM-10 est une des classifications élaborées par l'Organisation mondiale de la santé servant des buts globaux statistiques et de recherche et présentant ainsi de nombreux codes ne se rapportant pas à des diagnostics de maladies mais concernant des comportements déterminés („personnalité antisociale", „comportement d'opposition" de patients adolescents, „faute des parents en matière d'éducation", „appétits sexuels excessifs" ou „conflits avec les supérieurs"). En outre, les codes ne sont pas adaptés pour le contrôle des factures à plus d'un titre. La justification d'un moyen coûteux tel le scanner ne peut être contrôlée par un code de diagnostics connu par après, et le besoin d'un patient d'être hospitalisé dépend souvent plus de son environnement social que d'un diagnostic.

De plus le codage des informations augmente le danger que des diagnostics de suspicion ou d'exclusion soient considérés comme des diagnostics confirmés après leur transmission ou même inversés dans leur signification. Du reste des mécanismes coûteux devraient être mis en place pour rendre les codages transparents pour les patients.

Par ailleurs la durée de conservation et le but de l'utilisation des données par les assureurs ne sont à ce jour pas transparents, d'où danger d'utilisation abusive de ces données à d'autres fins.

La Conférence nationale des Préposés à la protection des données exige par conséquent que, d'une part, le flux soit limité aux données nécessaires et propres à atteindre le but recherché et, d'autre part, que l'on renonce à l'introduction prévue des codes CIM-10 pour le contrôle des factures. Afin de pouvoir assurer le secret médical, les contrôles des coûts et d'économicité ne doivent pas être effectués par assuré mais par cas. De la sorte, les services administratifs des assureurs ne seront pas saturés par des transferts de données inutiles, ni le secret médical mis en question. Il pourrait même s'agir d'une contribution active à la limitation des coûts de la santé.

4. Clause de consentement concernant la parution d'annonces dans des services en ligne

Clause de consentement

conformément à l'article 13, 1er alinéa de la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1)

1. La société responsable de la parution de l'annonce s'engage à prendre toutes les mesures de protection des données commandées par les circonstances. Toutefois, vu le caractère particulier des services en ligne (notamment sur Internet), la société responsable de la parution de l'annonce ne peut garantir entièrement la protection des données. Pour les raisons indiquées ci-dessus, l'annonceur est conscient des risques d'atteinte à sa vie privée inhérents à la parution de données personnelles dans de tels services accessibles à tout un chacun:

   1.1. les données personnelles sont accessibles également dans des pays n'ayant pas de législation équivalente à la législation suisse,

   1.2. la confidentialité des données personnelles n'est pas garantie,

   1.3. l'intégrité des données personnelles n'est pas garantie,

   1.4. l'authenticité des données personnelles n'est pas garantie,

   1.5. la disponibilité des données personnelles n'est pas garantie.

2. L'annonceur peut en tout temps révoquer son consentement.

Après avoir pris connaissance des points 1. et 2., le soussigné autorise, conformément à l'article 13, 1er alinéa de la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1), la société
.....
à faire paraître dans le service en ligne (site Internet)
.....
l'annonce faisant l'objet du présent contrat.

Lieu et date: Signature:
....

5. Communication de données concernant les chômeurs aux autorités de poursuite. Protection des données. JAAC 1997 III p. 664 ss.

- En raison de la particulière sensibilité des données concernant les chômeurs, les autorités d'exécution de l'assurance-chômage sont soumises à une obligation générale du secret. Une communication de données concernant les chômeurs à des autorités de poursuite sans accord écrit des assurés est exclue par la réglementation exhaustive des exceptions. Cette réglementation vaut comme lex specialis par rapport à l'art. 91 al. 5 LP.

Pour le solde du texte voir pages 104 ss

6. RECOMMANDATIONS DU PREPOSE FEDERAL A LA PROTECTION DES DONNEES

Voir pages 109 ss