Préposé fédéral à la protection des données

Rapport d'activités 2000/2001

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 2000 au 31 mars 2001.

TABLE DES MATIÈRES

*: Version originale en allemand

*: Version originale en allemand

*: Version originale en allemand

AVANT PROPOS

La mise en réseau de l'information dans notre société et la multitude des possibilités offertes par Internet constituent aujourd'hui un risque supplémentaire pour la sphère privée. En effet, comme le montrent de nombreuses études et enquêtes, les nouvelles technologies sont à l'origine de l'utilisation incontrôlée des données personnelles par des tiers.

Les prescriptions légales actuelles et les systèmes d'autorégulation ne suffisent plus à garantir une protection adéquate des transmissions de données personnelles. Placer la conception que nous avons actuellement de la protection des données uniquement dans le cadre rigide des dispositions légales ne permet pas de répondre aux besoins en pleine évolution de la société de l'information. Il est donc temps de rechercher des solutions techniques permettant de protéger la sphère privée. Cela requiert néanmoins de la part des services multimédias qu'ils intègrent systématiquement les exigences de la protection des données au niveau technique.

Les mêmes technologies qui permettent de mémoriser, d'utiliser et de transmettre des données personnelles devront aussi être utilisées pour protéger la sphère privée. Les procédés techniques à mettre en œuvre à cet effet seront fondés sur le principe d'une utilisation économe des données, permettront le recours aux pseudonymes et aux procédures d'anonymisation, requerront en ligne le consentement de l'utilisateur pour la collecte et l'utilisation de ses données personnelles et permettront également d'exercer en ligne le droit d'accès.

Par ailleurs, les labels de qualité définissant des critères communs d'examen et d'évaluation des systèmes d'information sont aussi un moyen de protéger la sphère privée. Leur définition nécessite néanmoins une entente au niveau international afin de mettre en place un cadre applicable dans l'Europe toute entière. Ainsi, grâce à des labels de qualité impliquant une application objective des exigences de la protection des données, liés à une normalisation, la technologie apportera une contribution essentielle à la protection des données au niveau national et international.

Mais pour que la mise en œuvre technologique de la protection des données devienne réalité, il faut qu'elle soit acceptée et soutenue par tous les intervenants dans le processus de protection des données (utilisateurs, entreprises, Etat), qu'elle soit réalisable dans la pratique, qu'elle améliore la protection de la sphère privée et qu'elle soit économiquement supportable.

Odilo Guntern

REPERTOIRE DES ABREVIATIONS

AI	Assurance-invalidité
CC	Centrale de compensation
CCDJP	Conférence des chefs des départements cantonaux de justice et police
CCPCS	Conférence des commandants des polices cantonales de Suisse
CEDH	Convention européenne des droits de l'homme
CFMJ	Commission fédérale des maisons de jeu
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DOSIS	Système de traitement de données en matière de lutte contre le trafic illicite de stupéfiants
FAMP	Système de traitement de données en matière de lutte contre la fausse monnaie, la traite des êtres humains et la pornographie
FMH	Fédération des médecins suisses (Foederatio Medicorum Helveticorum)
GEWA	Système de traitement de données en matière de lutte contre le blanchiment d'argent
ISIS	Système de traitement de données relatives à la protection de l'Etat
ISOK	Système de traitement de données en matière de lutte contre le crime organisé
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAMal	Loi fédérale sur l'assurance-maladie
LBA	Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier
LFLP	Loi sur le libre passage
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
OAR	Organisme d'autorégulation
OFAS	Office fédéral des assurances sociales
OFP	Office fédéral de la police
ONU	Organisation des Nations Unies
OSCE	Organisation pour la sécurité et la coopération en Europe
PJF	Police judiciaire fédérale
RIPOL	Système de recherches informatisées de police
SAP	Service d'analyse et de prévention
SID	Système d'information relatif aux documents d'identité

I. THEMES CHOISIS

1. Affaires de police

1.1. Le projet de nouveau passeport suisse

Dans le cadre de la réalisation du nouveau passeport suisse, un projet de loi fédérale a été élaboré. Cette loi constituera notamment la base juridique du système d'information relatif aux documents d'identité (SID). Collaborant au «groupe de travail droit» ainsi qu'au «comité de pilotage» du projet documents d'identité de l'Office fédéral de la police, nous sommes intervenus à différents stades de ce projet. Nos interventions ont principalement portés sur la problématique des droits d'accès au système SID, sur le maintien du caractère administratif et non policier de cette banque de données ainsi que sur le processus de personnalisation et de confection des livrets de passeport.

Le Conseil fédéral a adopté le 28 juin 2000 le message concernant la loi fédérale sur les documents d'identité des ressortissants suisses. Cette adoption marque une étape importante dans le cadre de ce projet d'envergure sous l'angle de la protection des données. En effet, le projet de loi présenté au Parlement constituera la base juridique du système d'information relatif aux documents d'identité (SID) et remplacera les ordonnances actuelles sur les passeports et les cartes d'identité.

Dans le cadre des travaux préparatoires à l'élaboration de ce message, nombre de problèmes touchaient directement à la protection des données. Nous avons étroitement collaboré avec l'Office fédéral de la police (OFP) à la recherche de solutions, notamment en participant tant au «groupe de travail droit» que dans le «comité de pilotage» du projet documents d'identité. Les premières étapes de ces travaux nous ont amené à émettre des réserves sur les risques de voir le système SID ne plus jouer le rôle d'une banque de données administrative mais de devenir une banque de données de recherches policières en raison de certains accès envisagés en faveur d'autorités de police. Nous avons en outre attiré l'attention du Conseil fédéral sur cette problématique dans la procédure de co-rapport lors de l'ouverture de la procédure de consultation externe.

Au cours des travaux de remaniement du projet qui ont suivis la procédure de consultation externe, des modifications ont été apportées notamment en ce qui concerne les droits d'accès. Nous avons pris position sur la version finale du projet de message en soulignant que les accès par procédure d'appel accordés au corps des gardes-frontière, aux services de police désignés par les cantons ainsi qu'au service de police compétent de la Confédération désigné pour le

traitement des demandes de vérification d'identité émanant de l'étranger étaient limités à des finalités claires et ancrées dans la loi (uniquement pour les vérifications d'identité ou pour l'enregistrement des pertes de documents) et nous paraissaient conformes au principe de proportionnalité. Tel que cela ressort clairement du message, ces accès ne devront en effet être utilisés qu'à des fins de contrôles quotidiens des documents d'identité dans le cadre de la détection des usages abusifs.

Nous sommes également intervenus afin que figure clairement au niveau de la loi l'interaction entre le système d'information SID et le système de recherches informatisées de police RIPOL. Il a ainsi été prévu dans le projet de loi que d'une part toute perte d'un document d'identité devra être signalée à la police et enregistrée dans le système RIPOL et que d'autre part, le système RIPOL transmettra automatiquement l'avis de perte au système SID.

Enfin, dans le cadre de l'adjudication de la conception du nouveau passeport, nous avons soutenu les choix des Départements fédéraux de justice et police, respectivement des finances, d'attribuer d'une part la conception des livrets de passeport à une entreprise privée tout en maintenant d'autre part la personnalisation et la réalisation du passeport à l'intérieur de l'administration fédérale. En effet, l'entreprise choisie pour ce mandat fournira les différents éléments du nouveau passeport tels que le papier, le matériel de couverture et les éléments de sécurité ainsi que les machines servant à la production. Par contre il appartiendra à l'Office fédéral des constructions et de la logistique de procéder à la personnalisation et à la confection des passeports. Cette solution garantit aux citoyens une production indépendante et sûre des documents au sein de la Confédération dès lors que les données personnelles resteront en mains des organes fédéraux et ne seront pas transmises en outsourcing à une firme privée.

Nous allons poursuivre nos tâches d'accompagnement et de conseil dans le cadre de ce projet, notamment par un suivi des débats parlementaires et la participation à d'éventuelles auditions en commissions et par l'élaboration de prises de position relatives au projet d'ordonnance en cours d'élaboration à l'OFP.

1.2. Les projets de réorganisation Strupol et Usis

Afin de réexaminer les structures de fonctionnement des autorités policières suisses, deux projets ont été mis sur pied. Sous l'appellation de projet «Strupol», l'Office fédéral de la police a reçu mandat de revoir les structures des différents services de police de la Confédération. D'autre part, dans le cadre du projet «Usis», un groupe de projet mandaté par le Département fédéral de justice et police et la Conférence des chefs des dépar-

tements cantonaux de justice et police a été chargé d'analyser le système global de la sûreté intérieure de la Suisse. Ces deux projets ayant de fortes implications au niveau des traitements de données effectués par les autorités policières, nous avons été invités à y participer.

Le groupe de projet «Strupol» a eu principalement pour objectif d'analyser l'intégration optimale des nouvelles fonctions attribuées à l'Office fédéral de la police (OFP), notamment dans le cadre du transfert à l'OFP de la Police fédérale et du Service de sécurité de l'administration fédérale jusqu'alors intégrés au Ministère public de la Confédération. Dans le cadre de ces travaux, nous sommes intervenus régulièrement à titre de conseil en mettant en évidence notamment les conséquences juridiques (modifications de lois et d'ordonnances) que certaines variantes de restructuration envisagées impliquaient. Nous avons également signalé la nécessité d'examiner les conséquences de ces projets sur les traitements de données effectués par les différentes unités policières en regard des normes légales en vigueur et des autorisations d'accès octroyées.

Les résultats des travaux ont abouti à une restructuration de nombreux services au sein de l'OFP ainsi qu'au transfert de différentes unités dans d'autres offices (tel que par exemple le transfert à l'Office fédéral de la justice du casier judiciaire, de l'entraide judiciaire et des extraditions). Ces modifications ont nécessité de nombreuses adaptations d'ordonnances du Conseil fédéral que nous avons examinées sous l'angle de la protection des données.

Sur la base des résultats du projet «Strupol», le Département fédéral de justice et police (DFJP) a décidé d'attribuer différemment les tâches de renseignement et de police criminelle assumées par la Police fédérale et les Offices centraux de police criminelle. Ainsi, un nouveau Service d'analyse et de prévention (SAP) recueillera, en application de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, des informations relatives notamment au terrorisme, à l'extrémisme violent et au commerce illicite d'armes. Il procédera à des évaluations de ces informations à l'attention des autorités politiques et de poursuite pénale. D'autre part, une nouvelle Police judiciaire fédérale (PJF) se chargera de toutes les procédures d'investigations préliminaires et d'enquêtes de police judiciaire relevant de la compétence fédérale. Cette nouvelle structure, entrée en vigueur le 1er janvier 2001, fera encore l'objet de notre part d'une attention soutenue, s'agissant en particulier de la répartition des traitements de données entre les différentes unités policières.

Le projet «Usis» quant à lui dépasse le cadre des mesures de réorganisation prises au sein de l'OFP. Mandaté par le DFJP et la Conférence des chefs des départements cantonaux de justice et police (CCDJP), le groupe de projet «Usis» a été chargé de réexaminer le système global de la sûreté intérieure de la

Suisse. Il a notamment pour tâche d'analyser la répartition des compétences policières entre la Confédération et les cantons.

Le groupe de projet s'est pour l'instant attaché à établir une analyse de la répartition actuelle des tâches policières et des charges financières. Nous avons pour notre part rappelé que toute modification envisagée dans la collaboration policière devait également être analysée à la lumière des bases légales réglant les échanges de données personnelles entre autorités de police. Nous avons aussi rendu attentif le groupe de travail «droit» sur la nécessité d'examiner concrètement quels systèmes informatiques de police seront touchés par le projet «Usis». Ce groupe a entamé un examen des compétences policières fédérales et cantonales, recensé la législation en vigueur et procédé à une première analyse des éventuelles normes qui devraient être révisées ou élaborées, notamment pour des raisons de protection des données.

Parallèlement au projet «Usis» de la CCDJP, un autre projet est mené sous l'appellation «Police XXI» par la Conférence des commandants des polices cantonales de Suisse (CCPCS). Ce projet vise à recueillir le point de vue des cantons sur la collaboration qu'ils pratiquent entre eux, mais aussi avec la Confédération et l'étranger. Dans le courant 2000, le calendrier du projet «Usis» a dès lors été modifié afin de pouvoir y intégrer les résultats du projet «Police XXI». Pour notre part, nous allons poursuivre notre collaboration au sein du projet «Usis» afin de veiller à ce que les exigences de la protection des données soient prises en compte dans le cadre des réorganisations policières envisagées.

1.3. Traitements de données dans le domaine des jeux de hasard et des maisons de jeu (casinos)

Lorsqu'ils remettent leurs demandes de concession, les casinos doivent entre autres fournir des indications détaillées sur les membres du conseil d'administration ainsi que sur les employés directement intéressés à l'exploitation des jeux. Etant donné que la loi sur les jeux de hasard et les maisons de jeu n'est entrée en vigueur que le 1er avril 2000, il n'est pas possible à l'heure actuelle d'avoir un avis définitif stipulant quels renseignements sont proportionnels. Il s'agit de déterminer quelles données sont nécessaires pour assurer une exploitation sûre et transparente des jeux. Il faut en outre s'assurer que ces données contribuent à éviter la criminalité et le blanchiment d'argent dans ou par les maisons de jeu. Une nouvelle appréciation de la situation devrait être faite dans deux à trois ans.

Le 1er avril 2000, la loi fédérale sur les jeux de hasard et les maisons de jeu (loi sur les maisons de jeu) est entrée en vigueur. Les maisons de jeu disposaient de six, respectivement douze mois pour déposer leur demande de concession auprès de la Commission fédérale des maisons de jeu (CFMJ) à l'intention du Conseil fédéral. Nous avons reçu plusieurs demandes en rapport avec les documents et renseignements exigés de la part de la CFMJ.

Dans un des cas, nous étions appelés à examiner quels sont les renseignements qu'une personne employée dans un casino doit fournir dans le cadre de la demande de concession. Dans sa fonction, la personne en question était chargée de compter l'argent, de changer de la monnaie ou des devises étrangères et de verser des chèques pour des montants supérieurs à 200.- gagnés avec les appareils à sous. Selon la CFMJ, cette personne était considérée comme «personnel associé à l'exploitation des jeux» et fut ainsi appelée, conformément à l'ordonnance sur les maisons de jeu, à fournir un curriculum vitae minutieux et à remplir un questionnaire détaillé de la CFMJ. Il fallait dans ce contexte tenir compte du fait qu'une vérification doit être effectuée lors de l'octroi de la concession que le casino est en mesure de garantir une exploitation des jeux sûre et transparente et que la lutte contre la criminalité et contre le blanchiment d'argent dans et par les maisons de jeu est assurée. Il s'avéra cependant qu'il est très difficile de constater quels documents et renseignements font partie d'un curriculum vitae minutieux et/ou sont nécessaires et appropriés (principe de la proportionnalité) pour assurer la surveillance de l'exploitation des jeux et ce faisant d'éviter le blanchiment d'argent. Ceci est d'autant plus vrai que la loi sur les maisons de jeu n'est entrée en vigueur que le 1er avril 2000 et qu'il n'a pas encore été possible de faire beaucoup d'expériences. Après avoir examiné les renseignements et les documents demandés, nous avons conclu que ceux-ci étaient pour la plupart en accord avec les dispositions de la législation sur la protection des données. Nous avons cependant attiré l'attention de la personne sur quelques points qui à notre avis appelaient certaines réserves. Nous avons néanmoins conseillé à la personne en question de remettre tous les documents demandés. Nous avons fait remarquer à la CFMJ qu'il serait opportun de procéder à une nouvelle appréciation de la situation dans deux à trois ans. Celle-ci devrait alors examiner quelles données sont vraiment nécessaires et appropriées pour atteindre les buts poursuivis, en particulier celui de la lutte contre le blanchiment d'argent.

Dans un autre cas nous fûmes amenés à étudier la question de savoir quels renseignements et documents certaines catégories de personnes – tels que les membres d'un conseil d'administration – devaient fournir. Selon la loi sur les maisons de jeu, ces personnes doivent jouir d'une bonne réputation et offrir la garantie d'une activité commerciale irréprochable. Les documents exigés pour établir la preuve de la bonne réputation sont mentionnés dans l'ordonnance sur les maisons de jeu. Il existait et existe donc une base légale pour la demande des

documents mentionnés, raison pour laquelle nous n'avions pas d'objection à formuler à ce propos. La CFMJ demandait en outre une liste de tous les mandats de conseil d'administration des membres du conseil d'administration des maisons de jeu. La CFMJ argumentait que ceci faisait partie intégrante d'un curriculum vitae d'un membre du conseil d'administration. Elle se basait dans son argumentation sur la pratique exercée par la Commission fédérale des banques. C'est la raison pour laquelle nous n'avions également rien à objecter contre la remise des documents exigés. Nous avons cependant, comme dans les autre cas, fait remarquer à la CFMJ qu'il serait nécessaire de procéder à une nouvelle appréciation de la situation après un certain temps.

Finalement, nous avions à étudier quels documents la CFMJ peut demander dans le cadre de sa fonction de surveillance. Cette tâche de la CFMJ consiste à vérifier si la maison de jeu a observé l'obligation de communiquer à laquelle elle est soumise. Cette vérification n'est cependant possible que si la CFMJ peut exiger les mêmes documents que ceux qu'elle a demandés lors de l'octroi de la concession. Au cas où la CFMJ aurait besoin – pour assumer sa tâche de surveillance – d'autres données personnelles qui ne sont prévues ni dans la loi sur les maisons de jeu, ni dans l'ordonnance qui s'y rapporte, il faudrait créer les bases légales correspondantes.

1.4. Expériences avec le droit d'accès indirect

Le droit d'accès «indirect» est prévu d'une part dans la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure pour le système de traitement de données relatives à la protection de l'Etat (ISIS). D'autre part, il vaut également selon la loi sur les offices centraux de police criminelle de la Confédération (LOC) pour les systèmes JANUS (anciennement DOSIS, ISOK et FAMP) et GEWA. En ce qui concerne la procédure à suivre pour exercer ce droit, nous avons dans les deux cas fait de nouvelles expériences.

L'année passée, nous avons à nouveau reçu plusieurs demandes de renseignement «indirectes». Nous avons remarqué à ce propos que le nombre de demandes déposées pour le système de traitement de données relatives à la protection de l'Etat (ISIS) en application de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) a légèrement diminué ces derniers temps. Par contre, le nombre des demandes de renseignement «indirectes» fondées sur la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) a augmenté. D'autre part, de plus en plus de personnes exercent leur droit d'être renseigné aussi bien selon la LMSI que selon la LOC.

Dans notre dernier rapport d'activités (voir 7ème rapport d'activités 1999/2000, pages 139 ss) nous avions déjà relevé que nous avions élaboré – en étroite collaboration avec les diverses unités de l'Office fédéral de la police (OFP) – une procédure claire et uniforme réglant le déroulement de l'exercice de ces droits d'accès «indirects». Les expériences que nous avons faites à ce propos avec les organes concernés varient. Nous tenons également à relever que les systèmes ISOK, DOSIS et FAMP des Offices centraux de police criminelle ont été réunis le 1er juillet 2000 en un seul système d'information baptisé JANUS. Ceci n'a cependant aucune influence sur l'exercice des droits d'accès.

La collaboration avec la Police fédérale (Service d'analyse et de prévention depuis le 1er janvier 2001) qui est responsable du système ISIS fonctionne sans problème. La procédure uniforme élaborée a été appliquée à tous les cas de demandes.

Pour les demandes de renseignement fondées sur la LOC, la vérification auprès de l'autorité de contrôle en matière de lutte contre le blanchiment d'argent pour le système GEWA s'est déroulée sans problème. En ce qui concerne le système JANUS par contre, nous avons adressé une recommandation aux Offices centraux de police criminelle de la Confédération leur demandant de rectifier certaines irrégularités. Il s'agissait entre autres d'un document qui n'avait pas été saisi ainsi que d'un document introuvable. Nous avons surtout attiré l'attention dans notre recommandation sur le fait que les Offices centraux de police criminelle de la Confédération devraient appliquer la même procédure que la Police fédérale. L'OFP a accepté la recommandation. Il a rectifié les irrégularités relevées et rédigé un résumé écrit de la procédure à appliquer. Les demandes d'accès «indirectes» encore en suspens ont alors pu être examinées.Le système JANUS est un système d'information uniquement. Cela signifie que tous les documents sous forme papier ne sont pas forcément saisis dans le système. D'autre part, certaines informations sont directement entrées dans le système par les cantons sans que l'OFP reçoivent une copie des documents. Dans ces conditions, l'OFP ne peut pas garantir que lors de l'examen des demandes toutes les données personnelles de la personne concernée qui sont traitées par les Offices centraux de police criminelle de la Confédération puissent être vérifiées. Le droit d'accès indirect ancré dans la LOC se réfère pourtant aussi bien au système d'information JANUS qu'aux documents sous forme papier. C'est pourquoi nous avons fait remarquer à l'OFP qu'il devait trouver une solution qui permette une application intégrale du droit d'accès tel qu'il est défini dans la LOC.

2. Télécommunications et poste

Télécommunications

2.1. Surveillance étatique des télécommunications et de la correspondance postale

La nouvelle loi fédérale sur la surveillance de la correspondance par poste et télécommunication qui entrera en vigueur vraisemblablement encore cette année est dans l'ensemble conforme aux principes généraux de protection des données. Elle s'appliquera à tous les organismes étatiques, aux organismes soumis à concession ou à l'obligation d'annoncer qui fournissent des services postaux ou de télécommunication ainsi qu'aux fournisseurs d'accès à Internet dans les cas de surveillance par poste et télécommunication ordonnée et mise en œuvre dans le cadre d'une procédure pénale fédérale ou cantonale.

La Sous-commission «Surveillance téléphonique» instaurée par la Commission des affaires juridique du Conseil national en novembre 1998 (voir 6ème rapport d'activités 1998/1999, pages 204-206) a rendu une année plus tard un rapport contenant un projet de rechange au projet du 1er juillet 1998 du Conseil fédéral. Les grandes lignes de ce projet de rechange sont les suivantes:

- le champ d'application de la loi est réduit, la possibilité de procéder à une surveillance pour prévenir un délit tombe et la surveillance du trafic des paiement de La Poste est calqué sur celui des banques;
- le catalogue des délits permettant une surveillance est sensiblement réduit, seuls les délits d'une gravité particulière ou dans la commission desquels la correspondance postale ou les télécommunications jouent un rôle clé sont retenus;
- les conditions dans lesquelles une surveillance est possibles sont plus restrictives;
- la pose de raccordements directs est réglé par la loi, une telle surveillance est autorisée que si elle ne porte pas atteinte à des intérêts prépondérants de tiers;
- la surveillance des personnes habilitées à refuser de témoigner pour raison de secret professionnel est en principe interdite, les exceptions à cette règle sont définies précisément dans la loi;
- le contrôle effectué par l'autorité qui autorise la surveillance de l'autorité qui l'ordonne est renforcé.

Nous avons soutenu ce projet de rechange tenant mieux compte des intérêts dignes de protection des personnes concernées.

Le Conseil national a adopté le projet de rechange proposé par sa Commission des affaires juridiques en décembre 1999. Lors de l'examen du projet de loi par le Conseil des Etats, sa Commission des affaires juridiques a proposé, entre autres, l'introduction d'une nouvelle disposition. Celle-ci obligerait les fournisseurs de services de télécommunication à identifier les usagers et fournir sur demande les données de trafic et de facturation durant au moins deux ans après l'ouverture d'une relation commerciale dans le domaine de la téléphonie mobile avec leurs clients n'ayant pas souscrit d'abonnement. Cette proposition a été adoptée en juin 2000 par le Conseil des Etats. En septembre 2000, le Conseil national a maintenu sa position de ne pas enregistrer les utilisateurs de téléphones portables avec cartes à prépaiement. Par la suite les deux Conseils ont maintenu cette divergence et en octobre 2000, la Conférence de conciliation a proposé d'adhérer à la décision du Conseil national. Cette proposition a été adoptée. Nous sommes d'avis que l'identification et l'enregistrement des acheteurs de cartes à prépaiement dans le domaine de la téléphonie mobiles ne sont ni nécessaires ni aptes à atteindre le but recherché, à savoir la lutte contre la criminalité. La mise en place de tels traitements de données supplémentaires, entraînant de nouveaux risques d'abus, ne répond pas au principe de la proportionnalité. Nous avons défendu cette position une nouvelle fois en février 2000 devant la Sous-commission «Surveillance téléphonique» de la Commission des affaires juridiques du Conseil des Etats.

La nouvelle loi fédérale sur la surveillance de la correspondance par poste et télécommunication entrera en vigueur vraisemblablement encore cette année. Elle remplacera les normes correspondantes contenues dans la législation fédérale sur la procédure pénale. Il faut signaler que la nouvelle loi s'appliquera non seulement à la surveillance de la correspondance par poste et télécommunication ordonnée et mise en œuvre dans le cadre d'une procédure pénale fédérale mais également dans le cadre d'une procédure pénale cantonale. Une telle surveillance ordonnée et mise en œuvre lors de l'exécution d'une demande d'entraide pénale internationale tombe également sous le coup de la nouvelle loi. Cette dernière s'applique non seulement aux fournisseurs de services postaux et de télécommunications, mais également aux fournisseurs d'accès à Internet.

Poste

2.2. Les formules de réexpédition de la Poste et la mise à jour des adresses (La Poste/DCL)

Le débat qui dure déjà depuis belle lurette autour du problème des demandes de réexpédition de la Poste et de la mise à jour des adresses a fait des progrès au cours de

l'année écoulée. La Poste a finalement accepté de ne mettre à disposition de tiers, pour la mise à jour des adresses, les données collectées par le biais des demandes de réexpédition que si le client de la Poste donnait son accord. Nous avons principalement critiqué la différence de prix énorme que devait subir les clients qui s'opposaient à une mise à jour des adresses ainsi que les explications en partie difficilement compréhensibles que l'on trouve sur les formulaires.

La Poste suisse propose à ses clients qui changent de domicile de profiter de la prestation de service «Demande de réexpédition d'envois» (voir également le 7ème rapport d'activités 1999/2000, pages 152 ss). Il suffit alors de remplir un formulaire avec la nouvelle adresse pour que le courrier soit automatiquement réexpédié au nouveau domicile. La réexpédition du courrier postal adressé à une ancienne adresse qui n'est plus valable occasionne des frais élevés, raison pour laquelle la Poste entreprend tout ce qu'elle peut pour qu'un maximum d'expéditeurs de courrier postal soient informés le plus rapidement possible de la nouvelle adresse afin qu'ils puissent d'emblée utiliser l'adresse correcte. La Poste propose – en collaboration avec l'entreprise Data Care AG – la prestation de service «MAT[CH]move» qui met à jour les adresses postales.

Au début de l'année 2001, la Poste a introduit de nouveaux formulaires qui permettent «officiellement» aux clients de refuser la mise à jour de leurs adresses auprès de tiers. Ceci répond à une exigence que nous avions formulée depuis longtemps. Il suffit maintenant que le client coche une case pour faire part de sa décision. S'il décide de ne pas accepter la mise à jour auprès de tiers, le client doit payer une taxe plus élevée.

L'année passée, le Conseil fédéral a – à la demande de la Poste, respectivement du DETEC – modifié l'ordonnance sur la poste. Celle-ci mentionne maintenant de manière explicite que «la Poste peut mettre les adresses postales de ses clients à la disposition de tiers pour la mise à jour par ceux-ci de leurs propres listes d'adresses, à condition toutefois que la personne concernée ne se soit pas expressément opposée au traitement de ces données». Cette disposition ne donne cependant pas de possibilités de traitements supplémentaires des données à la Poste car elle se borne à décrire les exigences en matière d'obtention du consentement qui sont déjà prévues dans la loi sur la protection des données.

Dans un souci de rendre les choses plus claires pour les clients, nous avons proposé à la Poste des versions plus compréhensibles des indications figurant sur ces formulaires. On y parle par exemple de l'«expéditeur» qui peut faire mettre à jour des adresses. Mais cette mise à jour d'adresses est à la portée de quiconque, tout à fait indépendamment du fait qu'il ait l'intention d'envoyer un courrier ou qu'il ait des intentions qui poursuivent des buts non postaux.

Nous avons informé la Poste du fait que nous n'approuvions pas l'énorme différence de prix imposée aux clients qui refusaient une mise à jour de leurs adresses auprès de tiers. Alors que ceux-ci payaient 10 francs par an jusqu'à fin 2000 pour la réexpédition, cette taxe est montée à 20 francs par mois en 2001, ce qui représente une augmentation de prix d'un facteur 24 ou de 2 300 %. Il est certes justifié de demander plus, étant donné que la Poste doit effectivement fournir un effort supplémentaire dans les cas où la mise à jour a été refusée. D'un autre côté, une différence aussi excessive viole le droit à l'autodétermination individuelle en matière d'information. Nous avons donc été contraints dans ce cas de formuler une recommandation à l'encontre de la Poste. La Poste a rejeté notre recommandation et nous avons porter l'affaire pour décision auprès du DETEC.

Relevons finalement qu'une personne qui change de domicile ne doit pas obligatoirement faire une demande de réexpédition auprès de la Poste. Elle peut également – bien que cela exige plus de travail – communiquer elle-même sa nouvelle adresse aux personnes, entreprises et autorités concernées. Sans demande de réexpédition, tout envoi adressé à l'ancienne adresse sera retourné à l'expéditeur avec la mention que le destinataire est inconnu à l'adresse indiquée.

3. INTERNET et technologies de la vie privée

3.1. Violation de la protection des données dans l'Internet

L'Internet nous confronte presque journellement à des violations plus ou moins graves de la protection des données. Nous vous présentons ci-après quelques exemples.

- Chez un fournisseur d'accès Internet, les noms d'utilisateur et mots de passe des comptes de messagerie électronique ont été accessibles par l'Internet. Ceci a eu pour conséquence que les données ont été récoltées par les moteurs de recherche qui présentèrent ces données comme résultats d'opérations de recherche. Les données ainsi divulguées permirent non seulement de lire le courrier électronique des personnes concernées, mais également d'envoyer et de supprimer des messages. Après que la brèche ait été découverte par un journaliste, l'entreprise concernée a immédiatement corrigé la faute. En fait, la panne avait été rendue possible par une erreur de configuration lourde de conséquences qui a existé plusieurs semaines sans que l'entreprise elle-même ne s'en rende compte. Cet incident a mené l'entreprise à revoir ses mesures techniques et organisationnelles.

- Plusieurs clients d'une banque apprirent par la presse que les informations concernant leurs paiements bancaires ainsi que leur adresse étaient librement accessibles sur l'Internet. Il ne s'agissait cependant nullement d'une brèche de sécurité du système de transactions bancaires électroniques de la banque concernée. Les données avaient involontairement été injectées dans un espace test qui était prévu pour héberger des données fictives et qui dès lors n'était délibérément pas protégé. Cet incident démontre que même les mesures techniques les plus sophistiquées au niveau de la sécurité ne peuvent empêcher que des données sensibles soient transférées dans un domaine du réseau qui est explicitement prévu pour un accès public (espace test, forum, site Web etc.). Comme on le sait, l'erreur est humaine et ne pourra jamais être complètement évitée. Il est cependant nécessaire que les déroulements soient conçus de sorte à ce qu'une seule erreur ne puisse pas à elle seule provoquer une catastrophe, mais qu'il soit possible de la déceler, si nécessaire en introduisant plusieurs niveaux de contrôle.

- Cette année nous avons à nouveau dû intervenir auprès d'exploitants de caméras Web. Il arrive régulièrement que de telles caméras soient installées dans des lieux publics (rues ou places). Etant donné qu'il n'est pas possible d'obtenir le consentement des personnes concernées qui se trouvent à ces endroits, les caméras doivent être réglées (angle de prise de vue, résolution) de manière à ce que les personnes ne puissent pas être identifiées.

3.2. P3P – une base technique pour l'autoprotection de ses données

La norme technique «Platform for Privacy Preferences Project (P3P)» est une base importante permettant à tout un chacun de protéger ses propres données sur Internet. Grâce à la P3P, les navigateurs de réseau contrôleront automatiquement si les préférences de protection des données introduites par l'utilisateur concordent avec la pratique du prestataire Internet.

P3P est une norme technique mise au point par le World Wide Web Consortium (W3C). Son intégration aux offres Internet et aux navigateurs de réseau permet aux utilisateurs de décider s'ils désirent livrer des données personnelles les concernant et lesquelles. Si l'offre Internet présente une déclaration de protection des données, l'utilisateur reçoit automatiquement une communication sur la manière dont ses données personnelles seraient traitées sur cette offre. L'utilisateur reçoit en outre un avertissement si les traitements de données du site ne concordent pas avec ses préférences d'utilisation.

Pour que cette norme déploie toute son efficacité, il faut qu'elle soit utilisée sur Internet par les exploitants de sites Web et les prestataires de services. Car si un prestataire n'a pas une offre compatible avec P3P, le contrôle automatique ne fonctionne pas. En effet, P3P ne peut fonctionner sans environnement technique adapté.

Nous estimons que P3P est un moyen technique utile pour les utilisateurs du réseau. Il constitue un précieux auxiliaire pour la personne qui désire contrôler l'utilisation de ses données personnelles. Il lui donne en effet la possibilité de savoir quelles sont celles qui ont été utilisées, quel en est le volume et comment elles l'ont été. Les traitements de données gagnent en transparence et, par conséquent, la confiance de l'utilisateur à l'égard des entreprises en ligne s'en trouve renforcée. Nous conseillons pour cette raison aux prestataires et entreprises d'élaborer sur Internet des déclarations de protection des données standardisées et lisibles automatiquement, fournissant aux utilisateurs et aux clients potentiels une information claire sur l'utilisation de leurs données.

4. Commerce électronique et protection des données

4.1. Eléments nécessaires pour l'octroi d'un label de qualité dans le commerce électronique du point de vue du droit de la protection des données

La portée mondiale du commerce électronique implique un échange massif de données personnelles, susceptible dans certaines circonstances de porter atteinte à la sphère privée. Il est donc très important que les principes fondamentaux de la protection des données soient aussi appliqués au commerce électronique.
En effet, si l'on veut renforcer la confiance de l'utilisateur dans le commerce électronique, les prestataires doivent assurer la transparence du traitement des données, ce qui est d'ailleurs une des conditions posées par la LPD. Ils doivent informer les utilisateurs des données personnelles qu'ils vont traiter et dans quel but. Dans ce contexte, nous saluons la création d'un label de qualité qui garantit entre autres un traitement de données personnelles conforme à la protection des données et renforce ainsi la confiance des clients dans le commerce électronique.

La procédure relative à l'octroi d'un label de qualité exige en premier lieu que les principes posés par la loi en matière de protection de la sphère privée soient appliqués à l'aide d'une norme technique. Pour qu'un label de qualité soit effi-

cace, il doit répondre, du point de vue du droit de la protection des données, aux exigences et critères d'examen suivants:

L'attribution d’un label de qualité doit reposer sur un processus transparent

L'attribution d’un label de qualité doit reposer sur un processus transparent, assorti de critères d'examen clairs. Il convient donc de garantir que la procédure d'attribution d’un label de qualité et les critères de qualité soient clairement définis et fixés dans le cadre d'une norme obligatoire. Le processus de certification ainsi clairement établi doit être alors suivi de l'attribution du label de qualité par une institution apte à cela dans le cadre d'une procédure d'audit.

Respect et application des principes généraux de protection des données

Avant d'attribuer le label de qualité, il convient de vérifier, grâce au processus de certification, que le traitement des données personnelles a bien lieu dans le respect des exigences légales. C'est la raison pour laquelle il convient de vérifier notamment les exigences suivantes:

- Assurer une information transparente à l'utilisateur ou au client (par ex. par une déclaration de traitement de données).
- Satisfaire aux exigences légales applicables au traitement de données (par ex. les critères de conservation, d'effacement et de transmission de données personnelles).
- Octroyer un droit d’accès et de rectification ainsi qu'un droit d'agir en justice en cas de litige ou de violation de la personnalité.
- Octroyer à l'utilisateur ou au client le droit de choisir s'il désire ou non que ses données soient utilisées.
- Garantir la sécurité des données par des mesures techniques et organisationnelles.

Processus de contrôle obligatoire avec sanctions et mesures en cas de non-respect des règles

Après l'attribution du label de qualité, un contrôle ultérieur, par ex. annuel, doit avoir lieu sur la base d'un processus sûr et obligatoire. Si les règles et exigences légales ne sont pas respectées, il convient de prévoir aussi des sanctions et des mesures, comme par exemple le retrait du label de qualité.

Respect des exigences européennes en matière de protection des données

Il convient également de tenir compte des exigences légales européennes en matière de traitement de données personnelles pour que le label soit valable au niveau international.

4.2. Mécanismes de règlement des litiges en cas de transactions en ligne (commerce électronique)

Les principaux critères permettant la bonne mise en œuvre de mécanismes parallèles pour le règlement en ligne des litiges sont répertoriés page 221.

5. Personnel

Secteur privé

5.1. Dépistage de drogues chez les apprentis

Le Préposé fédéral à la protection des données a publié, en collaboration avec plusieurs services spécialisés, un rapport (www.edsb.ch) présentant les conditions auxquelles doivent être soumis les tests de dépistage de la consommation de drogues chez les apprentis. En l'absence d'un intérêt prépondérant au titre de la sécurité et d'un consentement de l'apprenti, de tels tests sont absolument prohibés.

Depuis quelques années, le Préposé fédéral à la protection des données (PFPD) et d'autres services spécialisés constatent qu'un nombre toujours plus grand d'entreprises pratiquent des tests de dépistage de la consommation de drogues auprès des apprentis. Un groupe de travail a donc été constitué dans le but de concevoir des directives uniformes autorisant, dans le respect de la personnalité de l'apprenti, la prévention et la mise à jour de la consommation de drogues. Outre le PFPD, le groupe de travail réunissait l'Institut suisse de prévention de l'alcoolisme et autres toxicomanies (ISPA), le Secrétariat d'Etat à l'économie, l'Office fédéral de la santé publique et l'Office fédéral de la justice. L'Institut de médecine légale de Lausanne, les offices de la formation professionnelle ainsi que des représentants des employeurs et des employés ont également été consultés. Les conclusions du rapport sont exposées ci-dessous.

La consommation de drogues peut compromettre la sécurité au travail, diminuer les performances, influer sur le climat au sein de l'entreprise et occasionner des coûts. Dans certains cas, pour protéger ses intérêts, l'employeur recourt à des analyses d'urine (appelés aussi tests de dépistage) permettant de détecter s'il y a consommation de drogues. L'analyse d'urine, qui est un acte médical, constitue une atteinte à la personnalité de la personne examinée. Seul un intérêt prépondérant en matière de sécurité vis-à-vis de la protection de la personnalité, assorti

du consentement de l'apprenti, est à même de justifier un test de dépistage. L'employeur est habilité dans de tels cas à ordonner un test de dépistage.

Néanmoins, les tests de dépistage de la consommation de drogues ne libèrent pas l'employeur du devoir de prendre les mesures nécessaires à la sécurité du travail. Ces tests ne revêtent donc qu'un caractère complémentaire. Ils doivent être effectués par un médecin indépendant de l'entreprise et librement choisi par l'apprenti. Par contre, l'apprenti doit donner son consentement préalable lorsque le choix se porte sur le médecin de l'entreprise. S'il n'est pas d'accord, il peut choisir un autre médecin. De plus, il doit être informé du but et des conséquences du test. L'apprenti ne peut être obligé à donner son consentement, mais dans ce cas il doit s'attendre à supporter les éventuelles conséquences contractuelles. Il convient de noter que le consentement doit être libre, spécifique et exprès; enfin, pour que ce consentement soit valable, il faut que l'apprenti ait été informé du but et des conséquences du test.

En l'absence d'un intérêt prépondérant en matière de sécurité, les tests de dépistage de la consommation de drogues constituent une mesure disproportionnée. Le consentement à lui seul ne constitue pas un motif justificatif car sans intérêt prépondérant en matière de sécurité, la protection de la personnalité prime sur les autres intérêts de l'employeur. Exceptionnellement, le consentement peut constituer un motif justificatif valable lorsque le test de dépistage est dans l'intérêt de l'apprenti. Les tests de dépistage constitueraient une atteinte disproportionnée à la sphère personnelle de l'apprenti en l'absence d'un intérêt prépondérant en matière de sécurité surtout parce que la sécurité peut aussi être garantie avec efficacité grâce à d'autres mesures. S'il constate des problèmes ou des changements de comportement préoccupants chez l'apprenti, l'employeur peut le convoquer à des entretiens, fixer des buts concrets et des mesures, offrir son aide et menacer l’apprenti de sanctions s’il ne respecte pas les buts convenus. L'employeur est habilité à exiger que l'apprenti se soumette à une expertise médicale si cette mesure est nécessaire au recrutement de celui-ci ou à son maintien au poste qu'il occupe. Le consentement de l'apprenti est toutefois indispensable. La décision du médecin et le consentement de l’apprenti (rapports médecin-patient) déterminent si, dans le cadre de cette expertise, un test de dépistage sera effectué et si des questions relatives à la consommation de drogues seront posées. Dans le cadre de l'expertise médicale, l’employeur n’est habilité ni à exiger ni à proposer qu’on procède à un test de dépistage de la consommation de drogues.

Le médecin n'a le droit de communiquer à l'employeur que le constat relatif à l'aptitude de l'apprenti à occuper le poste en question. Il n'est pas habilité à lui donner des indications sur une éventuelle consommation de drogues (secret médical, ainsi que principe de la proportionnalité et principe de finalité).

On peut tout au plus concevoir que, dans le cadre d'un programme d'accompagnement global de l'employeur, le médecin soit habilité à transmettre certaines autres informations indispensables, à condition que l'apprenti y ait consenti. Dans ce cas, l'indication que l'apprenti consomme de la drogue doit permettre à l'employeur de prendre des mesures d'aide comme la mise sur pied de programmes de prévention, participer éventuellement au financement d'une thérapie de désintoxication. Si l'intérêt en matière de sécurité n'est pas prépondérant, l'employeur ne doit donc pas focaliser son attention sur la drogue, mais bien plus s'intéresser à l'ensemble des problèmes liés à sa consommation et à ses conséquences. Ce n'est que dans ces circonstances que l'on peut parler d'un devoir d'assistance élargi de l'employeur vis-à-vis de l'apprenti. Les tests de dépistage ont un caractère répressif alors qu'ils devraient servir de mesures de soutien; ils n'apportent donc aucune solution globale au problème de la drogue chez les jeunes et sont susceptibles de se solder par d'autres problèmes comme la discrimination de l'apprenti.

Si l'apprenti ne donne pas son consentement au test de dépistage ou ne désire pas que les résultats du test soient soumis à l'employeur et en l'absence d'un intérêt prépondérant en matière de sécurité, il ne devra pas en découler pour lui des conséquences négatives en droit du travail. Seule la constatation réitérée que les buts de l'apprentissage ne peuvent être atteints ou que l'apprenti n'a pas le contrôle de la consommation de drogues peut mener à des conséquences contractuelles. L'employeur doit considérer comme confidentielles les données éventuellement traitées en relation avec la consommation de drogues.

Au terme d'un examen de la situation actuelle dans les entreprises, le PFPD a constaté d'une part que certains employeurs procèdent à des dépistages de la consommation de drogues en accord avec les directives décrites ci-dessus (cf. également le 6ème rapport d'activités 1998/1999, page 257), mais que d'autres, partisans de la ligne dure, procèdent à des tests de dépistage en l'absence de tout intérêt prépondérant en matière de sécurité. Nous avons donc émis une recommandation à leur encontre (voir page 242). Ces derniers ont rejeté notre recommandation et nous avons porter l'affaire devant la Commission fédérale de la protection des données pour décision.

5.2. La surveillance du courrier électronique et d'Internet sur le lieu de travail

Nous avons récemment publié un schéma indiquant dans quelles circonstances l'utilisation d'Internet et du courrier électronique sur le lieu de travail pouvait être surveillée. Ce schéma met particulièrement l'accent sur la prévention technique. L'examen des données personnelles figurant dans les fichiers journaux n'est possible que s'il y a eu

constatation d'un abus. Par ailleurs, les données personnelles contenues dans les fichiers journaux ne peuvent être examinées que si l'employé concerné en a été auparavant informé. Le schéma en question figure page 239.

La prévention technique oui, la surveillance non: telle est, en résumé, la ligne de conduite qui devrait guider l'employeur quant à la sauvegarde de ses ressources. Les mesures techniques de protection garantissent entre autres la sécurité des données et des applications et protègent l'entreprise des surcharges du système. Parmi les mesures concrètes, citons la mise en œuvre de pare-feu (firewall) et de programmes antivirus, ou la limitation de la capacité de mémoire des utilisateurs. Les programmes destinés à surveiller les activités sur le réseau de certaines personnes (mouchards) ne sont pas autorisés. L'employeur comme l'employé doivent veiller par exemple à éviter l'introduction de virus ou les surcharges de capacité. Pour l'employeur, cela signifie essentiellement prendre les mesures de protection technique nécessaires. Les employés sont en revanche obligés d'agir avec la précaution requise lorsqu'ils surfent sur Internet ou reçoivent des messages électroniques d'inconnus.

Les activités des utilisateurs d'Internet sont enregistrées au fur et à mesure dans les fichiers journaux sous forme de données indiquant qui a visité quel site et quand. Ces fichiers journaux permettent donc d'identifier l'utilisateur.

L'employeur doit informer les employés des mesures techniques de protection prises, de la tenue d'un fichier journal, du règlement d'utilisation et des mesures de surveillance. Le règlement d'utilisation est un document qui détermine si l'usage d'Internet et de la messagerie électronique est permis et à quelles conditions. Il peut autoriser sans restriction l'utilisation d'Internet et du courrier électronique, la limiter (par exemple à la pause de midi), ou l'interdire totalement. L'employeur est en droit de contrôler si cette réglementation de l'utilisation est respectée à condition qu'un règlement de surveillance ait été rédigé. Nous recommandons avec insistance d'établir un tel règlement d'utilisation pour que soit clairement défini ce qui est autorisé et ce qui ne l'est pas.

Pour sa part, le règlement de surveillance énumère les contrôles auxquels les employés peuvent être soumis. Il les informe de la manière dont les données personnelles sont communiquées aux supérieurs hiérarchiques et des sanctions que ceux-ci sont à même de prendre. Les contrôles personnels ne sont autorisés que s'il existe un règlement de surveillance écrit et si un abus a été constaté lors d'un contrôle anonyme. Les contrôles personnels à titre préventif ne sont pas autorisés. Il y a abus si l'employé viole le règlement d'utilisation ou, en l'absence de règlement d'utilisation, s'il enfreint le devoir de loyauté vis-à-vis de son employeur ou contrevient au principe de la proportionnalité. On entend par devoir de loyauté l'obligation qu'ont les employés de défendre les intérêts de

l'employeur. Par exemple surfer exagérément durant les heures de travail est considéré comme disproportionné et comme un manquement au devoir de loyauté. Dans ce cas, un examen des données personnelles figurant dans les fichiers journaux est autorisé, bien entendu encore uniquement s'il existe un règlement de surveillance.

Normalement, ce n'est pas le supérieur hiérarchique qui procède à la surveillance, mais les services informatiques ou des préposés spéciaux à la sécurité. Ceux-ci communiquent les résultats des contrôles aux supérieurs hiérarchiques uniquement dans le cadre du règlement de surveillance.

S'il y a abus sans dérangement technique, l'examen des données personnelles figurant dans les fichiers journaux n'a lieu, pour des raisons de proportionnalité, qu'après la constatation d'un second abus. L'employeur doit donc informer les employés qu'il a constaté un abus et qu'un examen des données personnelles sera effectué si cela se reproduit.

Relevant de la sphère privée de tout un chacun, le contenu des messages électroniques privés demeure interdit à l'employeur. Même si l'usage privé du courrier électronique est interdit sur le lieu de travail, l'employeur n'est pas en droit de lire les messages électroniques de ses employés. Si, au cours d'un contrôle ponctuel, on soupçonne qu'un employé n'a pas respecté l'interdiction de faire usage du courrier électronique à titre privé, la constatation doit être faite sur la base du destinataire du message. En cas de doute sur le caractère privé ou non du message, il convient d'interroger directement l'employé.

Si la surveillance permet à l'employeur de soupçonner concrètement un acte délictueux, il ne peut enquêter que de manière limitée. La poursuite relève exclusivement de la justice pénale et l'employeur ne peut sauvegarder les moyens de preuve que s'il y a dénonciation de la personne soupçonnée. Si le soupçon porte sur un acte délictueux, l'employeur lui-même peut, pour des raisons de proportionnalité, constater l'identité de la personne soupçonnée, indépendamment du fait qu'il y ait ou non un dérangement technique. Des mesures de surveillance préventives plus poussées relèvent de la compétence des autorités pénales. S'il ne veut pas procéder à une dénonciation, les règles de la surveillance relevant du droit du travail et les sanctions y relatives demeurent valables.

Si un employé estime avoir été contrôlé par l'employeur de manière non autorisée, il peut déposer une plainte civile contre son employeur pour violation de la personnalité. S'il veut déposer une plainte pénale contre l'employeur, il doit le faire auprès des autorités compétentes pour violation de la sphère privée ou pour collecte non autorisée de données personnelles. En règle générale, l'employé dépose plainte auprès de la police.

Nous avons également publié sur notre site (www.edsb.ch) un guide détaillé sur ce sujet.

5.3. Traitement de données médicales par l'employeur

Une assurance-maladie a publié un CD-ROM destiné à contrôler les absences des employés. Ce CD-ROM contrevient aux principes de la protection des données. Formellement refusée, notre recommandation a néanmoins été appliquée.

L'examen de l'état de fait a montré que le CD-ROM en question permet à l'employeur de relever de manière systématique des données personnelles telles que nom, prénom, nationalité, motif de l'absence, médecin consulté, diagnostic, remarques etc. Ces données peuvent être exploitées en fonction de critères tels que la nationalité, le médecin ou le diagnostic, ou d'après des valeurs-cibles établies (budget-temps pour les maladies). De plus, ce CD-ROM facilite l'échange de données avec d'autres bases de données. Selon les indications fournies par l'assurance, le CD-ROM permet aussi à l'employeur de contrôler les absences de ses employés. Il est par ailleurs censé favoriser la protection de la santé et réduire les absences au travail. Pour l'essentiel, l'assurance est d'avis que l'employeur est en droit de traiter systématiquement les diagnostics de maladie afin d'obtenir une vue d'ensemble des absences des personnes en question et pouvoir décider s'il continue à garder un employé malade. Elle précise néanmoins qu'il n'y a pas d'échange de données avec des banques de données de l'assurance.

Nous estimons que le CD-ROM constitue un traitement de données disproportionné et inapproprié car l'employeur n'a pas besoin de relever systématiquement les données concernant la santé de ses employés pour être en mesure d'exécuter le contrat de travail. En vertu du principe de la proportionnalité, il est particulièrement inadmissible que l'employeur ou son service du personnel relèvent de manière systématique les diagnostics médicaux. Le relevé systématique de ces diagnostics n'est requis ni par des mesures de prévention dans le domaine de la santé, ni par la gestion des absences, ni par la décision concernant le maintien ou non d'un collaborateur malade à son poste. Uniquement de cas en cas, dans la mesure où l'établissement des faits le requiert, l'employeur ou le service de prévention de la santé et de la sécurité de l'entreprise ou de la branche concernée peuvent prendre connaissance des causes de la maladie d'une personne déterminée. Sans consentement explicite de l'employé, l'employeur n'est en droit de ne traiter qu'un avis médical («malade» ou «apte/pas apte pour un poste»). Par contre, il est permis de relever le nombre de jours d'absence pour maladie, sans autre spécification.

Le traitement de données tel qu'il est ici prévu est également à critiquer du fait que les données médicales peuvent être combinées et comparées avec d'autres données personnelles comme la nationalité par exemple. Il est possible, à notre avis, d'en tirer des conclusions discriminatoires. Nous n'avons pas constaté sur le relevé systématique par l'employeur d'autres motifs d'absence (par ex. vacances, service militaire etc.), ce que permettrait aussi le CD-ROM.

Il est également inapproprié de qualifier le CD-ROM de mesure médicale. La législation sur le travail oblige l'employeur à prendre les mesures nécessaires afin de prévenir les dangers pour la santé de ses employés. Les locaux de travail, systèmes et machines doivent être entretenus de manière à ce que leur utilisation ne puisse pas avoir de répercussions sur la santé des employés. La saisie d'informations sur les «points faibles» dans l'entreprise (courants d'air, substances dangereuses, fumée, écrans de mauvaise qualité etc.) a lieu de manière anonyme, sur la base de données statistiques. Uniquement de cas en cas, dans la mesure où cela est nécessaire pour établir les faits dans un cas spécial, l'employeur ou le service de prévention de la santé et de la sécurité de l'entreprise ou de la branche concernée peuvent prendre contact avec la personne directement impliquée. En revanche, le CD-ROM dont il est ici question est uniquement un instrument destiné au contrôle des absences.

L'établissement d'un budget annuel des jours de maladie est également inadmissible, car il peut donner lieu à une discrimination à l'égard des personnes faibles de santé qui sont souvent absentes. L'affirmation de l'assurance selon laquelle le traitement de données en question ne serait pas discriminatoire à leur égard du fait que des budgets «maladie» individuels peuvent être établis pour ces employés, va à l'encontre des objectifs de la réduction des absences.

Il est certes possible qu'il n'y ait pas d'échange de données entre l'assurance et l'employeur, comme l'assurance l'affirme. Mais cela ne change rien au fait qu'uniquement la possibilité technique d'un tel échange de données est contraire à la loi. Ni le consentement de la personne concernée, ni une base légale, ni un intérêt prépondérant privé ou public ne sont donnés pour qu'il puisse y avoir échange d'informations entre la banque de données des absences et d'autres banques de données. Du reste, sans motif justificatif, une communication de données de cette sorte constituerait une violation du secret professionnel de la part de l'employeur.

Sur la base de ces considérations, nous avons recommandé à l'assurance d'interrompre immédiatement la production et l'exploitation du CD-ROM en question et de retirer les CD-ROM déjà en circulation ou d'enlever les catégories discutables de données du CD-ROM. L'assurance ne s'est pas déclarée d'accord avec nos considérations, mais a remanié le CD-ROM en conformité avec la protection des données.

6. Assurances

Assurances sociales

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

L'Office fédéral des assurances sociales (OFAS) est chargé d'examiner si les centres de désintoxication peuvent bénéficier de subventions de l'AI ou non. Pour ce faire, l'OFAS a besoin entre autres de données médicales concernant les patients traités dans ces centres. Le volume des données qu'il conviendrait de fournir soulève néanmoins des questions (cf. également le 7ème rapport d'activités 1999/2000, pages 170-171).

L'OFAS conclut des contrats de prestations avec les centres de désintoxication. Ces institutions doivent répondre à certaines conditions pour pouvoir bénéficier de subventions de l'AI. En particulier, 50 % de leurs résidants doivent être des handicapés au sens de la législation sur l'assurance-invalidité. L'OFAS demande de ce fait à ces centres de lui fournir entre autres des données médicales sur les personnes concernées. Or les données sur la santé sont des données personnelles sensibles. Nous avons donc signalé plusieurs fois à l'OFAS que la collecte de données sensibles requiert les bases légales nécessaires.

Il convient de considérer que les centres de désintoxication sont en premier lieu des institutions qui fournissent un suivi ambulatoire à des toxicomanes ou d'anciens toxicomanes surtout et traitent à ce propos des données très sensibles. En raison de la sensibilité de ces données, il convient aussi de soumettre les principes régissant leur traitement à des exigences plus strictes, en particulier pour ce qui est du principe de la proportionnalité. L'une des possibilités est de transformer les données personnelles des personnes concernées en données anonymes. On peut pour cela utiliser les codes grâce auxquels les données sont «pseudonymisées». L'utilisation de pseudonymes ne peut toutefois pas être effectuée par le destinataire, mais doit être entreprise par le centre de traitement, par exemple en attribuant un numéro de patient. Les données qui sont transmises sous forme codée doivent être réduites à un minimum. L'OFAS recevrait ainsi des données uniquement munies du code utilisé par le centre de désintoxication. Quoi qu'il en soit, dans un cas précis et sur la base d'une demande concrète, le client serait à nouveau identifiable.

6.2. Fonds des caisses de pension: recherche des ayants droit

La Centrale du 2e Pilier a pour mission de rendre les «avoirs oubliés» des caisses de pension à leurs ayants droit. La recherche des assurés, qui vivent pour la plupart main-

tenant à l'étranger, s'est révélée néanmoins très difficile. On a donc étudié les moyens de rassembler les adresses manquantes par d'autres voies et les bases légales nécessaires ont été modifiées en conséquence.

Tous les travailleurs n'ont pas fait valoir leurs droits en matière de fonds des caisses de pension. Ce sont dans la plupart des cas des travailleurs originaires d'autres pays d'Europe qu'il convient de rechercher et de trouver pour qu'ils puissent bénéficier de leurs droits. La réglementation prévue dans la loi sur le libre passage est néanmoins insuffisante. Il était en particulier impossible de trouver toutes les adresses par l'intermédiaire de la Centrale de Compensation (CC) de l'AVS. Il a donc été proposé de trouver les adresses manquantes en s'adressant aux autorités étrangères en charge des assurances sociales. Le PFPD a recommandé d'adapter les bases légales en conséquence (cf. également le 7ème rapport d'activités 1999/2000, pages 166-167).

Pour ce qui est des travailleurs espagnols, un accord international (échange de notes) a été élaboré à cet effet entre la Suisse et l'Espagne. Cet accord établit qu'une fois par an, la Centrale du 2e Pilier transmet un support de données (nom, prénom et date de naissance des ayants droit non localisés de nationalité espagnole) aux autorités espagnoles d'assurances sociales. Celles-ci recherchent les travailleurs domiciliés en Espagne et informent la Centrale du 2e Pilier.

Il était important à nos yeux que les données ne soient traitées que dans ce but (principe de finalité). Par ailleurs, nous avons accordé une grande importance au fait que l'échange de notes contient aussi des dispositions sur la sécurité des données. Il y est en particulier et expressément mentionné que les supports de données doivent être transmis sous forme chiffrée.

Nous saluons cette réglementation et espérons que des solutions analogues seront également trouvées avec d'autres pays.

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

Le rapport final de la Commission d'experts sur la protection de la personnalité dans l'assurance-maladie et l'assurance-accidents sociales et privées a été présenté au Département fédéral de l'intérieur (DFI) en octobre 2000 et publié en mars 2001.

La commission a entamé ses travaux en mars 1998 et tenu au total 17 séances. Le groupe de travail avait entre autres pour mission de traiter les thèmes touchant à la protection de la personnalité dans l'assurance-maladie et dans l'assu-

rance-accidents sociales et privées. Concrètement, il s'agissait de mettre au point des propositions d'amélioration ainsi que des dispositions légales entièrement formulées. Du point de vue de la protection des données, les principes de la proportionnalité et de la transparence avaient la priorité.

Dans le domaine de l'assurance obligatoire des soins, il fallait entre autres déterminer les données dont les assureurs-maladie et les assureurs-accidents avaient besoin. Du point de vue du PFPD, il est important de mentionner à ce propos que les données sur la santé ne doivent être ni collectées, ni conservées afin de constituer des réserves de données (principe de la proportionnalité). Il convient donc de déterminer avec précision les données dont l'assureur a besoin et dans quels buts.

Dans le domaine des assurances complémentaires, les discussions ont notamment porté sur les formulaires d'adhésion comportant des questions sur l'état de santé, ainsi que sur la clause de consentement. En tout état de cause, les questions de l'assureur ne doivent pas violer la personnalité du requérant et doivent répondre au principe de la proportionnalité. La clause de consentement destinée à délier le médecin du secret professionnel doit être claire et reconnaissable pour la personne qui donne son consentement (cf. également 7ème rapport d'activités 1999/2000, pages 195-197).

Les questions sur la santé sont en principe autorisées en vue de l'admission dans l'assurance d'indemnité journalière pour maladie. Cette pratique est néanmoins susceptible de se traduire par une discrimination pour les employés porteurs de «risques élevés». En effet, l'employeur comme l'assureur ont dans ce cas un intérêt financier à ne pas engager ou à se défaire d'une personne dont l'état de santé serait inapproprié. Nous demandons donc l'abandon général des questions sur l'état de santé dans le domaine des assurances d'indemnité journalière pour maladie.

Actuellement, le système des médecins-conseils est réglé uniquement dans la LAMal. Plusieurs modèles ayant pour thème l'indépendance des médecins-conseils vis-à-vis des services administratifs des assurances ont été discutés. Le problème des échanges de données entre le médecin-conseil et les services administratifs des assurances a également été examiné. A nos yeux, il est important que le système des médecins-conseils soit étendu le plus possible à d'autres formes d'assurance. Il convient en particulier d'examiner sérieusement un système analogue dans le domaine de l'assurance-accidents.

Le rapport de la commission d'experts a été soumis au DFI en octobre 2000 et publié en mars 2001. Plusieurs de nos exigences ont été prises en compte, notamment l’utilisation de formulaires d’adhésion distincts pour l’assurance obligatoire des soins et pour l’assurance complémentaire.

Assurances privées

6.4. La nécessité du médecin-conseil dans le domaine de l'assurance privée

La fonction de médecin-conseil est réglementée dans le domaine de l'assurance-maladie et doit être saluée du point de vue de la protection des données. La personne assurée a la possibilité de ne communiquer ses données médicales qu'au médecin-conseil. La question se pose donc de savoir s'il convient aussi de mettre en place une institution analogue dans le domaine de l'assurance privée.

La fonction de médecin-conseil est réglée par la loi fédérale sur l'assurance-maladie (LAMal). Le médecin-conseil fait office de «filtre» en quelque sorte entre l'assuré et les services administratifs de l'assurance-maladie. Il conseille les assureurs sur les questions médicales ainsi qu'en matière de dédommagement et d'application des tarifs. Il examine en particulier les conditions auxquelles est soumis l'assureur quant à l'obligation de fournir sa prestation. Soulignons par ailleurs qu'il rend son avis de manière indépendante.

La question se pose actuellement de savoir s'il faut créer une fonction similaire dans d'autres domaines des assurances et mettre en place les bases légales nécessaires.

Dans le domaine des assurances privées, il existe depuis une quinzaine d'années des recommandations relatives au traitement des documents médicaux. Une de ces recommandations, élaborée par la FMH et les assurances privées, prévoit entre autres que les dossiers médicaux qui contiennent des données personnelles sensibles puissent être soumis au service médical ou au médecin-conseil de l'assureur. Par ailleurs, il est possible de demander que ces données soient conservées auprès de l'assureur dans un dossier à part. Les assureurs doivent également garantir que ces documents ne soient accessibles qu'à un nombre limité de personnes. En outre, ils doivent indiquer sur le formulaire de demande d'adhésion que des données sensibles peuvent être communiquées à l'adresse de l'assureur à l'attention du service médical ou du médecin-conseil (avec la mention «personnel»).

Les services médicaux ou les médecins-conseils ne sont donc pas une nouveauté dans le domaine des assurances privées et se sont révélés judicieux. Il serait néanmoins souhaitable qu'ils soient également indépendants vis-à-vis des assureurs.

Nous demandons donc que dans le domaine des assurances privées, la fonction des services médicaux et des médecins-conseils soit également réglée au niveau de la loi (tâche, but, organisation etc.). Les médecins-conseils sont d'autant plus importants en matière d'assurances privées que c'est justement un domaine où les discriminations en raison d'un état de santé inapproprié ne sont pas à exclure. Au cas où des analyses génétiques dans le domaine des assurances - que le PFPD rejette en principe - devraient néanmoins être un jour possible, le médecin-conseil s'imposera là aussi.

6.5. Les prises de sang ne sont pas du ressort des assureurs

Afin d'être en mesure d'apprécier leurs risques, les assureurs privés peuvent rassembler des données sur la santé des personnes désirant être assurées. Ils sont néanmoins liés par le principe de la proportionnalité. Il est donc exclu qu'un assureur demande des prises de sang.

Une personne s'est adressée à nous pour savoir si une compagnie d'assurance était habilitée à demander des analyses de sang dans le cadre de la procédure d'admission à une caisse de pension.

Une compagnie d'assurance peut demander des renseignements sur la santé d'une personne désirant être admise dans la mesure où ces renseignements sont effectivement nécessaires. Dans le domaine de la prévoyance professionnelle, les renseignements sur la santé ne peuvent être requis que pour ce qui va au-delà de l'assurance obligatoire. Certes, la compagnie d'assurance a le droit de demander les données nécessaires sur la santé de la personne en question (principe de la proportionnalité). Mais elle ne peut en aucun cas exiger des substances corporelles telles des échantillons de sang. Les données écrites fournies par le requérant ou le médecin traitant sont amplement suffisantes. Le requérant est tenu de dire la vérité; s'il ne respecte pas cette obligation, il commet une violation de l'obligation de déclarer. Le médecin est en outre lié par son devoir de vigilance médicale. Il serait donc disproportionné qu'un assureur demande encore au requérant des échantillons de sang ou d'urine, en plus des données sur sa santé.

Par ailleurs, on ne peut exclure le risque que l'assureur utilise les échantillons de sang pour d'autres buts, par ex. pour en extraire des informations génétiques. On ne sait pas non plus si ces données sont transmises au service médical de l'assurance ou même aux services administratifs de la même assurance. Une autre question se pose encore, à savoir qui doit avoir accès à ces données sensibles,

en quel lieu et combien de temps ces échantillons sont-ils conservés? Nous procédons actuellement aux éclaircissements nécessaires.

6.6. Transmission de données à des réassureurs

Les compagnies de réassurance demandent aux assureurs de leur fournir des données sur leurs assurés afin de pouvoir examiner le droit à la prestation. Il convient à cet effet de rendre les données des assurés aussi anonymes que possible.

Une compagnie de réassurance nous a soumis pour avis des extraits d'un règlement pour l'assurance des grands risques. Ce règlement établit que des copies et des certificats de personnes assurées peuvent être soumises au réassureur sous certaines conditions. Par ailleurs, le réassureur aurait le droit de demander d'autres documents aux assureurs ou de les consulter.

Du point de vue de la protection des données, il convient d'anonymiser autant que possible les données des assurés. La question se pose donc de savoir si la compagnie de réassurance a chaque fois besoin des données mentionnées ci-dessus. On pourrait envisager d'anonymiser les données à l'aide de codes qui seraient en possession des assureurs. Dans un cas concret, le réassureur pourrait accéder éventuellement aux données de l'assuré pour pouvoir examiner de plus près les droits aux prestations. Les données des assureurs seraient anonymes, mais pourraient être recomposées si nécessaire (pseudonimisation). Il convient par ailleurs de mentionner que le traitement des données personnelles nécessite la présence d'un motif justificatif. Si un réassureur traite les données d'un assuré privé, il faut en général le consentement concret des personnes assurées. Si un réassureur est également présent dans le domaine de l'assurance-maladie sociale, les réglementations de la communication de données spécifiques de la LAMal sont à prendre en considération.

6.7. Contrôles de qualité dans le domaine des assurances complémentaires

Dans le domaine de l'assurance complémentaire, les assurances-maladie cherchent à améliorer le contrôle de qualité des fournisseurs de prestations et, dans ce but, traitent des données personnelles. Ils sont tenus à cette occasion de respecter les principes de la protection des données.

Le PFPD est de plus en plus souvent confronté aux questions touchant le contrôle de qualité des fournisseurs de prestations dans le domaine des assurances complémentaires. Les caisses-maladie notamment constituent des associations qui ont pour but de contrôler la qualité des différents fournisseurs de prestations dans le domaine des assurances complémentaires. Des données personnelles sont relevées à cet effet sur les fournisseurs de prestations. Ceux-ci, par exemple les centres de fitness, doivent fournir de grandes quantités de données sur la formation du personnel, les mesures méthodiques etc. A cet égard, il est déterminant que seulement les données effectivement nécessaires soient collectées (principe de la proportionnalité). Il serait à nos yeux disproportionné que des représentants de caisses-maladie se rendent à l'improviste chez des prestataires de service. Il est du reste inutile de traiter les données personnelles des assurés dans le cadre d'un contrôle de qualité.

Par ailleurs, le traitement des données doit être transparent pour les fournisseurs de prestations. Ils doivent être informés de manière complète de ce qu'il advient de leurs données. Nous avons donc proposé de remettre un aide-mémoire sur la protection des données aux fournisseurs de prestations. En outre, les données ne peuvent être traitées que dans le but indiqué lors de la collecte (principe de finalité). Ce principe vaut en particulier pour les données qui contiennent des secrets commerciaux des fournisseurs de prestations. Les caisses-maladie ne peuvent traiter les données personnelles qu'en présence d'un motif justificatif. Si des données de fournisseurs de prestations sont traitées dans le domaine des assurances complémentaires, le consentement de ceux-ci est indispensable. La question demeure toutefois de savoir si le consentement du fournisseur de prestations peut avoir lieu librement. En effet, s'il veut demeurer reconnu de certaines assurances complémentaires, le fournisseur de prestations n'a en fait souvent pas d'autre choix que de se soumettre à un tel contrôle de qualité.

7. Santé

7.1. Centres d’appel dans le domaine médical

Dans le domaine médical, de plus en plus de centres d’appel sont mis sur pied pour offrir la possibilité à la population de s’informer lors d’un cas de maladie sur les premières mesures à prendre ou sur les démarches à faire. Lors de ces conversations téléphoniques, des données sensibles de l’appelant sont traitées. Ceci soulève les questions fondamentales de la transparence, du traitement de données, du consentement de la personne concernée ainsi que de la sécurité des données.

L'année écoulée a vu un grand nombre de centres d'appel médicaux surgir sur le marché. En fonction de leur spécialisation, ces centres d'appel offrent à l'appelant d'une part la possibilité d'obtenir des informations sur les premières mesures à prendre ainsi que sur les démarches ultérieures à entreprendre. D'un autre côté, les clients réguliers du prestataire du centre d'appel ont accès par exemple aux prestations de service suivantes: organisation de soins médicaux, information du personnel soignant à l'étranger ou établissement de plans de soins à long terme.

La majorité des contacts entre le patient et le centre d'appel ont lieu par téléphone. Pour pouvoir être conseillé, le patient doit fournir aux collaborateurs du centre d'appel un grand nombre d'informations sur son état de santé, informations qui sont traitées par le centre d'appel. Il est vrai que l'appelant sait en règle générale quelles sont les informations qu'il a fournies oralement au centre d'appel. On peut néanmoins se poser la question de savoir si l'appelant est également conscient de l'étendue des traitements que le centre d'appel effectue avec les données qu'il lui a fournies oralement. En règle générale, les conversations téléphoniques sont enregistrées. Les centres d'appel utilisent en outre divers logiciels plus ou moins sophistiqués qui permettent de saisir les informations fournies par téléphone. Ces programmes sont utilisés par les collaborateurs du centre d'appel comme aide à la décision et doivent leur faciliter leur tâche de conseil. Les données ainsi saisies restent enregistrées dans ces programmes pendant un certain temps, d'une part pour permettre d'assurer le suivi médical du client, d'autre part à des fins de conservation de preuves. La question se pose de savoir si l'appelant est conscient du fait que les conversations téléphoniques sont enregistrées et que les informations qu'il fournit oralement sont stockées et exploitées à l'aide de logiciels. Ce n'est que s'il connaît entièrement l'étendue des traitements effectués que l'appelant est en mesure de donner un consentement légalement valable. Si son consentement est légalement valable, les traitements effectués par le centre d'appel sont admissibles. Ce consentement peut être obtenu par écrit dans les cas où l'appelant est un client régulier du prestataire du centre d'appel. Ce qui pose problème par contre, c'est l'information détaillée préalable des personnes qui appellent le centre de manière spontanée. Le fait d'informer l'appelant que la conversation téléphonique est enregistrée ne suffit pas pour que ce dernier puisse se faire une image de la durée pendant laquelle les enregistrements sont conservés et des autres traitements de données qui sont en outre effectués en arrière-plan.

Reste à relever que ceci soulève diverses questions concernant la sécurité des données en rapport avec la possibilité de mise sur écoute du raccordement téléphonique du centre d'appel, des autorisations d'accès et des possibilités d'accès aux données par des personnes non autorisées.

7.2. Projets de mesure et d'assurance de la qualité dans le domaine médical

Pour des raisons d'économie de coûts, les hôpitaux, mais aussi les homes instaurent de plus en plus des projets permettant de mesurer et d'assurer la qualité. Ceci soulève des questions quant à la nécessité de traiter des données personnelles sensibles ainsi que sur la finalité, la transparence et le consentement des personnes concernées de même que sur la sécurité des données.

Selon la loi fédérale sur l'assurance-maladie (LAMal), le fournisseur de prestations est tenu de fournir ses prestations de manière économique et d'assurer leur qualité. C'est pourquoi les fournisseurs de prestations qui ont des déroulements plus complexes, tels que les hôpitaux ou les homes, mettent en œuvre des projets de mesure et d'assurance de la qualité. Selon leurs objectifs, ces projets servent à optimiser le rapport coût-efficacité en vue des soins à donner aux clients futurs, actuels ou aussi bien actuels que futurs. Afin de pouvoir mesurer et assurer la qualité, des informations sont saisies sur l'état de santé des clients, sur leurs habitudes quotidiennes, leur conception de la vie et leurs désirs.

Un des problèmes qui se pose dans ce contexte est la licéité des traitements de données personnelles. Etant donné que la LAMal ne prévoit pas explicitement que des données personnelles, en particulier des données personnelles sensibles et des profils de la personnalité, puissent être traités, la question se pose de savoir si le traitement des données est admissible après obtention du consentement légalement valable de la personne concernée. Pour des raisons de conservation de la preuve, il est judicieux et nécessaire d'obtenir ce consentement par écrit. Un consentement légalement valable doit être bien lisible, compréhensible et formulé de manière à ce qu'il informe le consentant sur les conséquences de son assentiment. Il doit en outre lui donner la possibilité de révoquer ce dernier en tout temps. Ce droit de révoquer à tout moment implique que le consentement doit avoir été donné de plein gré. Un tel consentement n'est pas légalement valable s'il a été obtenu dans des conditions où l'on a exercé une quelconque pression sur la personne concernée. Ceci englobe entre autres les pressions exercée sur des groupes de personnes («tout le monde doit donner son consentement…»), une pression d'ordre matériel («si je ne donne pas mon accord, mes frais ne seront pas pris en charge…») ou la menace d'une baisse de qualité possible («si vous n'êtes pas d'accord, vous ne pourrez pas non plus profiter des améliorations au niveau de la qualité…»).

La question se pose en outre, du point de vue de la proportionnalité, de savoir s'il est nécessaire de traiter des données personnelles. On entend par données personnelles toutes les informations concernant une personne identifiée ou

identifiable. Concrètement, la question est donc de savoir s'il est nécessaire pour procéder à l'analyse de la qualité d'utiliser des données qui identifient chaque client ou s'il serait possible d'utiliser des données rendues anonymes ou identifiées par un pseudonyme. Dans les cas où la mesure de la qualité et l'amélioration de qualité qui en résulte doit profiter directement à un client individuel actuel, il est certainement nécessaire de pouvoir à nouveau attribuer les données à dépouiller ainsi que les résultats à la personne dont on a analysé les données. Par contre, si les données sont traitées en vue d'une assurance et d'une amélioration future de la qualité, la situation est différente. Dans ce cas, l'amélioration de qualité ne profitera plus à la personne dont on a analysé les données. A notre avis, il n'est pas admissible dans ce cas d'utiliser des données personnelles pour effectuer ces analyses. Il suffit de travailler avec des données qui ont été préalablement rendues anonymes. Si l'on défend par contre le point de vue qu'il doit être possible de savoir sur une période prolongée quelles sont les prestations qui ont été fournies à une personne déterminée, nous somme d'avis qu'il faut utiliser des données pseudonymisées. Cela signifie que les éléments qui permettent d'identifier la personne concernée sont munis d'un code, que les prestations fournies à une même personne sont enregistrées sous ce même code et que le fichier des relations, c.-à-d. la base de données qui contient le lien entre le code et les éléments d'identification, est tenue séparément des données relatives aux prestations.

Il est fréquent que l'analyse des données à des fins de mesure et d'assurance de la qualité n'est pas faite par l'institution prestataire elle-même, mais déléguée à des entreprises externes. Nous sommes d'avis que dans ces cas seules des données anonymisées ou pseudonymisées doivent être communiquées à l'entreprise tierce et que, dans le cas des données pseudonymisées, cette entreprise ne doit pas avoir accès au fichier des relations. Cette obligation découle du degré élevé de protection qu'exigent les données médicales qui bénéficient en outre d'une protection supplémentaire par le biais des obligations de secret professionnel fixées par la loi, telles que le secret médical par exemple. Il est pensable que le système informatique attribue automatiquement un code au moment de la saisie des données personnelles. Ensuite, chaque fois que l'on saisirait les mêmes données d'identification, le système irait rechercher le même code. Ce procédé garantirait que les données appartenant à une même personne soient toujours assignées au même code. Les données ainsi rendues «anonymes» seraient ensuite transmises à l'entreprise tierce. L'analyse serait alors effectuée avec les données pseudonymisées.

Un autre aspect qui mérite d'être pris en compte dans le cadre des projets de mesure et d'assurance de la qualité est la question de la finalité des données traitées. Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre le but qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Si le client

n’est pas suffisamment informé sur le but poursuivi avant que les données soient collectées, on est en droit de douter que le principe de finalité soit respecté. Il y a lieu de différencier dans ce contexte également si la mesure et l’assurance de la qualité bénéficiera à nouveau au client dont on a traité les données. L’objectif primaire d’un traitement de données est de prodiguer des soins à un client. On peut dans ce cas admettre que la mesure et l’assurance de la qualité a un impact immédiat sur le suivi et les soins médicaux de la personne concernée. On peut donc admettre dans cette constellation que le principe de la finalité est respecté. La situation est à notre avis différente lorsque la mesure et l’assurance de la qualité ainsi que l’analyse des données sont effectuées pour en faire bénéficier des clients futurs qui se trouvent dans des situations comparables. Dans ces cas, le traitement des données personnelles n’est plus justifié par le but du suivi et du traitement médical.

Un autre aspect de la proportionnalité, mais également de la sécurité des données, est la gestion des droits d’accès aux données devant être dépouillées ou – dans le cas où les données ont été munies d’un pseudonyme – au fichier des relations. Eu égard à la sensibilité élevée des données et au fait que la violation du secret médical est pénalement répressible, il est nécessaire à notre avis de concevoir les procédures de manière à ce que seuls les médecins traitant ou le personnel médical auxiliaire responsable puissent saisir les données à l’aide de grilles de saisie clairement structurées, prévues pour l’analyse, par exemple en utilisant des système de codification et des logiciels appropriées. Les données munies d’un pseudonyme seraient alors mises à disposition des personnes qui sont responsables de les analyser. Cette démarche garantirait que seules les personnes autorisées manipulent les données personnelles sensibles. Ceci n’affecte en rien le respect du secret médical et du secret professionnel. Quant au fichier des relations, qui fait le lien entre une personne déterminée et un code, il ne serait pas accessible à des tiers.

Dans le cadre de l’application technique des droits d’accès par exemple au fichier des relations, nous conseillons de ne pas crypter uniquement les accès individuels aux données, mais bel et bien la base de données elle-même.

7.3. Ordonnances médicales sous forme électronique

L’idée d’utiliser des ordonnances médicales sous forme électronique est en train d’apparaître sur le marché. Cette idée soulève des questions quant au consentement du patient et à la sécurité des données.

A l’ère de l’informatique, la créativité quant aux possibilités d’utilisation de systèmes électroniques pour traiter des données personnelles semble ne pas

connaître de limites. Ainsi, des suggestions sont apparues sur le marché visant à remplacer l'ordonnance usuelle sous forme papier par une version électronique. La démarche proposée se présente ainsi: le patient se rend chez son médecin. Au terme de la consultation, le médecin lui prescrit un médicament. Au lieu de prendre son bloc d'ordonnances habituel, le médecin utilise un micro-ordinateur de la taille d'un bloc d'ordonnances. Il entre alors dans la grille affichée par ce micro-ordinateur toutes les indications qui étaient également nécessaires jusqu'ici pour délivrer une ordonnance. Il peut ensuite imprimer l'ordonnance et la remettre au patient. Le but de la saisie électronique est cependant de pouvoir transmettre l'ordonnance par voie électronique à la pharmacie que le patient aura choisie. L'ordonnance transmise depuis le micro-ordinateur du médecin arrive sur le serveur d'un distributeur (entreprise tierce). Celui-ci se charge de faire suivre l'ordonnance sur le serveur de la pharmacie indiquée. Le serveur de la pharmacie envoie alors un accusé de réception au serveur du distributeur qui à son tour confirme au médecin la transmission de l'ordonnance.

Pour une appréciation de projets de ce genre, nous attachons une importance primordiale à deux aspects: le patient doit donner son accord à la transmission d'une ordonnance électronique de plein gré et la sécurité des données doit être assurée.

Pour que le patient puisse donner son consentement, il doit préalablement être informé de manière détaillée et dans un langage qui lui est compréhensible sur les conséquences techniques et pratiques de l'acheminement électronique de l'ordonnance et il doit avoir la liberté réelle de décider si oui ou non il donne son accord à l'utilisation de l'ordonnance en version électronique. Le patient doit apprendre de manière claire quelles sont les personnes qui ont accès à ses données. Cela signifie en particulier que le patient doit être informé du fait que le distributeur (entreprise tierce) traite des confirmations de transmission. Le problème crucial au niveau de ces confirmations est la forme sous laquelle leur contenu est visible pour le distributeur. Une des possibilités est d'y inclure des données permettant une identification directe du patient et qui pourraient être lues par le distributeur. Le distributeur saurait alors qu'un patient donné a été en traitement chez un médecin donné. Une autre possibilité consiste à mentionner un numéro de patient attribué par le médecin qui ne permette pas au distributeur d'identifier le patient. A notre avis, seule la deuxième solution satisfait aux exigences du principe de la proportionnalité en excluant l'accès de personnes non autorisées à des données personnelles sensibles.

Un autre aspect important de la sécurité des données est la transmission sécurisée de l'ordonnance électronique. Etant donné que l'ordonnance permet par recoupement de connaître la maladie d'une personne et qu'il s'agit en conséquence de données personnelles sensibles au sens de la loi sur la protection des

données, les exigences envers la transmission pour éviter l'accès de personnes non autorisées doivent être très élevées (voir également page 199).

Nous sommes d'avis que les entreprises qui lancent de tels projets pour les mettre à disposition de leurs clients – dans ce cas des médecins et des pharmacies – doivent également assumer leur responsabilité qui consiste à appliquer les dispositions de la protection des données. Ils doivent notamment appliquer des mesures techniques et organisationnelles qui correspondent au niveau technologique actuel.

7.4. Facturation électronique - offices d'encaissement externes

Il existe plusieurs projets qui ont pour but de réaliser une facture électronique. L'idée est que la facture soit transmise par voie électronique du fournisseur de prestations à l'organisme payeur. A part le fait qu'ils sapent de manière insidieuse l'autoresponsabilité du patient, ces projets présentent des problèmes du point de vue de la protection des données. Citons entre autres la dégradation ou l'annulation du droit à l'autodétermination individuelle en matière d'information, la question de la proportionnalité des traitements de données et celle de la sécurité des données.

Actuellement, plusieurs représentants de milieux intéressés présentent sur le marché divers projets visant à réaliser une facture électronique. L'idée de base de tous ces projets est que le fournisseur de prestations envoie une facture électronique au payeur (assureur).

Nous avons dû constater qu'une tendance existe à inclure beaucoup plus de données relatives aux patients dans les formulaires de facturation électroniques que dans les versions papier. Si l'on admet que les indications mentionnées sur les factures qui jusqu'ici étaient imprimées et remises à l'assureur suffisaient pour le remboursement des coûts, on est en droit de se poser des questions sur la proportionnalité des données qui seraient traitées lors d'une facturation par voie électronique. Il est incompréhensible que les assureurs auraient tout à coup besoin de bien plus d'informations pour être en mesure de procéder au remboursement des frais. On est donc en droit de se demander si le fait que les moyens électroniques - permettant sans problème de traiter bien plus de données qu'auparavant avec les formulaires papier - ne suscitent des ambitions de traiter plus de données. Ceci a lieu bien que le volume des données ne soit pas absolument nécessaire pour l'accomplissement de la tâche prévue, à savoir le remboursement des frais. Nous sommes par ailleurs d'avis que le contenu et le volume des données ne doit pas différer selon que le débiteur auquel on envoie la

facture électronique soit le patient ou l'assureur. Aussi longtemps que le contenu est identique, il n'importe pas que la facture papier contienne les informations en clair alors que la facture électronique utilise un code.

Comme pour tous les projets dont le but consiste à transmettre des données personnelles sensibles, il faut veiller à ce que la transmission se fasse en utilisant les techniques les plus modernes (voir également page 199).

Si des entreprises tierces sont impliquées dans les déroulements et les flux de données, que ce soit comme distributeur ou dans le cadre d'un contrat de fiducie, les questions suivantes se posent: quelles sont les tâches concrètes qu'assume un tel office d'encaissement? Quelles sont les données auxquelles ces offices d'encaissement ont accès et qu'ils peuvent ainsi lire ou modifier? Pour quelle durée les données sont-elles conservées par ces offices d'encaissement? Les possibilités de traitement vont de la simple distribution où un accès aux données transmises n'est pas possible à l'exécution de tâches propres à l'assureur dans le cadre d'un contrat d'outsourcing.

A part les aspects mentionnés, les projets soulèvent également des problèmes de fond. Le principe fondamental du «tiers garant» statué dans la loi fédérale sur l'assurance-maladie qui considère que le patient est le débiteur et que c'est lui qui fait suivre la facture à l'assureur dans le cadre de sa propre responsabilité en matière de santé est sournoisement supprimé. D'autre part, il n'est plus clair pour le patient quels traitements de données sont effectivement effectués et quelle en est l'étendue. Le patient perd ainsi la possibilité d'exercer le droit d'autodétermination individuelle en matière d'information qui lui est conféré par la loi sur la protection des données. Il n'est plus en mesure d'intervenir étant donné qu'on lui enlève la possibilité de décider lui-même quelles données il désire transmettre à son assureur.

La question fondamentale se pose également à ce propos de savoir si le consentement du patient pour cette forme de traitement est suffisant du point de vue légal. Si ces projets devaient être adoptés par le marché, nous doutons que le caractère «de plein gré» tel qu'il est exigé par la loi pour l'obtention du consentement soit satisfait. Le pouvoir du «fait accompli» ne laissera plus le choix au patient de prendre une décision libre de toute contrainte. L'admissibilité légale de tels traitements est dès lors discutable.

7.5. Le tarif médical Tarmed

Les aspects importants à examiner du point de vue de la protection des données en rapport avec le tarif médical Tarmed sont l'indication du diagnostic détaillé sur la facture ainsi que la facturation électronique.

Même avec le nouveau tarif médical (Tarmed), l'utilisation de factures électroniques reste un point de discussion controversé. Nous renvoyons à ce sujet au thème précédent sur la facturation électronique et les offices d'encaissement externes (voir page 165).

Un des points contestés est de savoir s'il est admissible ou non d'inclure systématiquement des données de diagnostic détaillées sur les factures qui sont transmises à l'assureur. Nous sommes d'avis que, conformément à la loi sur l'assurance-maladie, la communication systématique d'un diagnostic «sommaire» est défendable et proportionnelle. Par contre, nous maintenons notre opinion que des communications systématiques de diagnostics détaillés ne sont conciliables ni avec la loi fédérale sur l'assurance-maladie, ni avec le principe de la proportionnalité. Comme les factures ne prêtent en règle générale pas au doute, le remboursement des frais peut avoir lieu sans problème. L'assureur peut par contre, dans des cas isolés dûment justifiés, demander des diagnostics plus détaillés ou des informations complémentaires s'il juge que la facturation nécessite des éclaircissements. Nous nous opposons à la collecte et au stockage systématique de données personnelles sensibles.

7.6. Procédés permettant de contrôler le caractère économique des prestations dans le domaine de la santé

Certains assureurs ont, dans le cadre des méthodes permettant de contrôler le caractère économique des prestations effectuées, transmis à des associations d'assureurs toutes les factures avec les données complètes des patients en provenance du fournisseur de prestations soumis au contrôle. Selon le principe de la proportionnalité, une identification du patient n'est défendable que dans des cas exceptionnels et isolés. Il suffit de pouvoir reconnaître quelles prestations ont été fournies pour une personne donnée.

Selon la loi fédérale sur l'assurance-maladie (LAMal), le fournisseur de prestations (médecin, hôpital, home, thérapeute) est tenu de fournir ses prestations de manière économique. Les assureurs sont tenus de contrôler ceci auprès des fournisseurs de prestations. Etant donné que les assureurs ne disposent pas en règle générale des capacités nécessaires pour procéder eux-mêmes à ces

contrôles, ils délèguent cette tâche aux associations cantonales d'assureurs. Pour ce faire, ils transmettent aux associations d'assureurs non seulement des données générales concernant le fournisseur de prestations telles que le nom, l'adresse, le numéro du fournisseur de prestations, la nature et l'étendue des prestations par catégories, mais également – et ceci de manière systématique – des données concernant le patient. Nous nous sommes opposés à cette pratique parce que nous la jugeons contraire au principe de la proportionnalité. La vérification du caractère économique concerne uniquement le fournisseur des prestations. Nous sommes d'avis qu'il suffit en principe pour atteindre ce but de pouvoir identifier toutes les prestations qui ont été fournies pour une personne donnée. Il n'est donc pas nécessaire que les associations d'assureurs sachent quelle est la personne qui a bénéficié de ces prestations. L'attribution de diverses prestations à une même personne pourrait être faite avec des données pseudonymisées. La méthode consisterait à attribuer à chaque patient un numéro sous forme de code. Les prestations seraient alors identifiées à l'aide de ce numéro et non plus avec le nom et l'adresse du patient. Les associations d'assureurs ne recevraient plus que les données pseudonymisées.

Etant donné que les associations d'assureurs n'appliquent pas de pratique unifiée en ce qui concerne la communication de données relatives aux patients, mais qu'il a néanmoins été reconnu en partie que les associations d'assureurs n'ont en principe pas besoin de connaître l'identité du patient pour procéder à la vérification du caractère économique des prestations, une des associations d'assureurs, le Concordat des assureurs-maladie suisses (CAMS), a demandé d'élaborer un régime unifié pour l'ensemble de la Suisse qui puisse être accepté par toutes les parties impliquées.

7.7. Remise du dossier médical aux patients

Il arrive de plus en plus souvent que des patients demandent à leur médecin non seulement qu'il leur permette de consulter leur dossier médical, mais également qu'il le leur remette. Nous continuons à partager l'avis que le dossier médical appartient au patient, mais que le médecin est chargé conformément aux dispositions légales de le conserver. Il importe donc de trouver des solutions praticables permettant de résoudre ce conflit.

Il arrive de plus en plus fréquemment que des médecins nous consultent parce que certains de leurs patients demandent non seulement une copie de leur dossier médical auquel ils ont droit dans le cadre du droit d'accès stipulé dans la loi sur la protection des données, mais exigent qu'ils leur remettent le dossier médical. Les médecins sont alors confrontés à un conflit puisque d'un côté les législations cantonales en matière de santé publique les obligent à conserver les

dossiers médicaux de leurs patients pendant plusieurs années et que d'un autre côté la législation sur la protection des données stipule que le dossier médical appartient au patient. L'obligation de conserver le dossier médical a entre autres été prévue pour permettre au médecin de disposer de preuves au cas où un patient formulerait à son encontre des revendications découlant de la relation établie dans le cadre du traitement. L'obligation de remettre le dossier par contre est issue du droit à l'autodétermination individuelle en matière d'information qui est ancré dans la loi sur la protection des données et qui stipule que toute personne a le droit de décider elle-même quelles données la concernant un tiers est autorisé à traiter.

Il s'agit de rechercher et de trouver une solution praticable qui permette de résoudre ce conflit. Comme nous l'avons déjà décrit dans notre guide relatif au traitement de données personnelles dans le domaine médical, la solution pourrait à notre avis consister à faire signer au patient au moment de la remise du dossier médical une déclaration dans laquelle celui-ci libère explicitement le médecin de son devoir légal et contractuel de conservation et renonce à toute prétention envers le médecin qui découle de la relation établie dans le cadre du traitement.

7.8. Transfert de données médicales par Internet

Si le transfert de données médicales par Internet est effectivement très simple et donc très tentant, il y a cependant lieu d'observer certaines règles de conduite permettant d'éviter des violations majeures en matière de protection de données. Il est également clair que la protection de ces données sensibles doit faire l'objet d'une attention extensive et ne se limite pas à leur seul transfert.

Depuis quelques années déjà, nous assistons à une intensification du transfert de données médicales sur Internet. Des échanges ont par exemple lieu entre patients et médecins, entre médecins eux-mêmes, entre médecins et laboratoires d'analyse, entre hôpitaux et médecins, entre prestataires de soins et assurances, entre assurés et assurances, entre employés et employeurs. De manière à éviter les risques de transmission de données sensibles à des tiers indésirables, il est recommandé de suivre les règles suivantes:

- s'enquérir de la licéité du transfert et n'échanger que des données exactes et indispensables
- pratiquer une anonymisation ou tout au moins une pseudonymisation des données à chaque fois que cela est possible. L'utilisation des initiales éventuellement accompagnées de l'année de naissance du patient, constitue une forme rudimentaire de pseudonymisation qui présente de grands risques

d'identification par des tiers et surtout d'erreur d'identification par le destinataire. Il faut donc plutôt recourir à une véritable pseudonymisation tel que le code de liaison «anonyme» développé pour l'Office fédéral de la statistique

- utiliser exclusivement des canaux de transmission sécurisés pour le transfert de données médicales se rapportant à des personnes identifiées ou identifiables. On utilisera ainsi le protocole HTTPS (avec clé de session d'au moins 128 bits) pour la communication avec des serveurs Web. S'agissant du courrier électronique, il est absolument indispensable de crypter, voire même de signer électroniquement, les informations échangées. On entre là dans le domaine des infrastructures à clés publiques (PKI: Public Key Infrastructure), pour lesquelles il existe de nos jours des solutions concrètes, efficaces et économiques (certification Swisskey, web-of-trust «Pretty Good Privacy»...).

Il va de soi que la sécurité et la protection ne doit pas se limiter au seul transfert des données. Une fois arrivées à bon port, celles-ci doivent continuer à être traitées de manière sûre et confidentielle. On veillera ainsi tout particulièrement aux données médicales sur ordinateur portable ou assistant digital personnel (PDA: Personal Digital Assistant), pour lesquelles une mémorisation sous forme cryptée s'impose. Les systèmes reliés directement à Internet doivent en outre disposer de remparts de protection appropriés (routeur, filtre, coupe-feu...) contre les attaques extérieures. Enfin, les données stockées sur des serveurs en réseau local doivent naturellement être protégées de façon à ce que seuls les ayants droit puissent y accéder.

Pour le futur, on tend vers la solution du dossier électronique du patient, contenant l'ensemble de son historique médical et géré de manière entièrement transparente pour lui.

8. Génétique

8.1. Loi sur l'utilisation de profils d'ADN

Nous avons salué l'élaboration d'un projet de loi sur l'utilisation de profils d'ADN, mais avons regretté que ce dernier ne fasse pas l'objet d'une consultation auprès des milieux intéressés (consultation externe). Lors de l'examen de ce projet, nous avons défendu les positions suivantes: le prélèvement de matériel génétique doit être ordonné par un juge et uniquement dans les cas prévus expressément par la loi (catalogue des délits); en cas de non-lieu ou d'acquittement, les profils d'ADN doivent être automatiquement effacés de la banque de données et le matériel génétique détruit.

Les traitements de données génétiques à des fins de recherches judiciaires et plus particulièrement la banque nationale de profils d'ADN ont pour base légale provisoire l'ordonnance sur le système d'information fondé sur les profils d'ADN. Au regard de la loi sur la protection des données, une telle base légale est insuffisante. En effet, ces traitements concernent des données sensibles. En mars 2000, nous ne nous étions pas opposés, sans toutefois l'approuver, à cette solution pour autant qu'une base légale formelle suffisante soit rapidement élaborée (voir notre 7ème rapport d'activités 1999/2000, pages 181-182). Le Département fédéral de justice et police (DFJP) a tenu son engagement en proposant au Conseil fédéral en octobre 2000 un projet de loi fédérale sur l'utilisation de profils d'ADN dans le cadre d'une procédure pénale et sur l'identification de personne inconnues ou disparues.

Le matériel génétique humain et les profils d'ADN sont beaucoup plus que de simples empreintes digitales ou photographies. En effet, il est possible de déduire du matériel génétique des informations sur les maladies, les maladies héréditaires et les prédispositions. On ne peut de même pas exclure que l'on puisse dans un avenir proche déduire des profils d'ADN également des informations sur les prédispositions voire même sur l'état de santé d'une personne. La conservation de matériel génétique et les banques de profils d'ADN comportent ainsi des dangers réels pour les droits fondamentaux des personnes concernées. C'est pourquoi il est nécessaire d'élaborer une réglementation plus stricte que celle relative à l'identification «ordinaire» (empreintes digitales et photographies). Le projet de loi transmis au Parlement contient plusieurs points problématiques:

Lors des discussions sur la nécessité de mettre en place une procédure de consultation externe, il a notamment été argumenté qu'une telle procédure avait déjà eu lieu dans le cadre du projet de loi fédérale sur l'analyse génétique humaine. Or ce projet de loi ne visait principalement pas l'utilisation des profils d'ADN dans le cadre d'une procédure pénale et l'infime partie touchant à ces aspects qui y étaient consacrés ne correspondait en rien au projet de loi transmis au Parlement. En raison des nombreuses inconnues liées aux analyses de profils d'ADN dans le cadre d'une procédure pénale et au caractère extrêmement sensible de ce domaine, nous sommes de l'avis qu'il aurait fallu procéder à une consultation externe.

D'autre part, l'établissement d'un catalogue des délits au niveau de la loi garantirait une utilisation restrictive de l'analyse de l'ADN dans le cadre de la procédure pénale contrairement au modèle proposé par le DFJP qui autorise la police à effectuer des prélèvements sans cadre légal clair. Nous avons également soutenu la nécessité d'élaborer un tel catalogue des délits au niveau de la loi pour les écoutes téléphoniques et la surveillance du courrier; c'est cette voie qu'a

choisie le Parlement lors de l'adoption de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication.

Les dangers susmentionnés légitiment le recours à un juge. Le prélèvement de matériel génétique sur l'ordre d'un juge ne met pas en péril le travail de la police. Dans un cas d'urgence, il est concevable que la police elle-même décide de procéder à un prélèvement. Une telle décision devrait par la suite être confirmée par un juge.

Nous soutenons également l'effacement automatique de l'inscription dans la banque de profils d'ADN et la destruction du matériel génétique en cas de non-lieu ou d'acquittement. L'intérêt de la personne accusé à tort à se retrouver dans la situation avant l'atteinte est supérieur aux arguments avancés par le DFJP (procédure d'annonce entre les autorités pénales et le service responsable de la banque de profils d'ADN jugée disproportionnée) pour un effacement à la demande de la personne concernée.

9. Finances

9.1. La loi sur le blanchiment d'argent et la reconnaissance d'intermédiaires financiers

Selon la loi sur le blanchiment d'argent, les intermédiaires financiers avaient un délai jusqu'au 1er avril 2000 pour s'affilier à une organisation d'autorégulation reconnue, faute de quoi ils seront soumis à la surveillance directe de l'autorité de contrôle en matière de lutte contre le blanchiment d'argent. Nous avons été appelé à vérifier si les documents demandés aux intermédiaires financiers par une telle organisation reconnue d'autorégulation étaient admissibles du point de vue de la loi sur la protection des données. Nous avons rendu attentif l'autorité de contrôle en matière de lutte contre le blanchiment d'argent qu'une nouvelle appréciation de la situation s'imposerait d'ici deux à trois ans.

La loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier (LBA) considère également comme intermédiaires financiers les personnes qui, à titre professionnel, acceptent, gardent en dépôt ou aident à placer ou à transférer des valeurs patrimoniales appartenant à des tiers. Celles-ci peuvent s'affilier à un organisme d'autorégulation reconnu (désigné ci-après par OAR) qui se chargera alors de surveiller l'intermédiaire financier. Les intermé-

diaires financiers qui ne s'affilient pas à un OAR sont soumis à la surveillance directe de l'autorité de contrôle en matière de lutte contre le blanchiment d'argent. Les intermédiaires financiers disposaient d'un délai de deux ans à partir de l'entrée en vigueur de la LBA (1er avril 1998) pour s'affilier à un OAR, faute de quoi ils seront soumis à la surveillance directe de l'autorité de contrôle.

Un intermédiaire financier nous a contacté en rapport avec sa demande d'affiliation auprès d'un OAR. Il était d'avis que les formulaires d'admission de cet OAR contenaient trop de questions personnelles. Nous avons tout d'abord constaté que la LBA exige des OAR qu'ils déterminent les modalités pour l'admission et l'exclusion d'un intermédiaire financier dans un règlement. Ce règlement doit à son tour être approuvé par l'autorité de contrôle en matière de lutte contre le blanchiment d'argent. Dans le cas cité, l'intermédiaire financier était appelé selon le règlement de l'OAR à prouver que les personnes chargées de l'administration et de la gestion jouissaient d'une bonne réputation dans ce domaine d'activité. Il devait en outre garantir par la mise en place d'une organisation d'entreprise adéquate qu'il était en mesure d'assurer l'exécution des obligations fixées dans la LBA. Les mêmes conditions sont d'ailleurs imposées par la LBA aux intermédiaires financiers qui sont directement subordonnés à l'autorité de contrôle.

Nous avons ensuite examiné si les documents demandés par l'OAR étaient proportionnels, c'est-à-dire s'ils étaient vraiment nécessaires et appropriés pour prouver la bonne réputation de l'intermédiaire. A notre avis, seuls les curriculum vitae signés ainsi que les diverses lettres de référence pouvaient éventuellement entrer en conflit avec le principe de la proportionnalité. Comme nous ne disposions cependant pas d'indices concrets, nous n'avons pas pu émettre d'avis sur cette question. Nous avons attiré l'attention sur le fait que dans le domaine bancaire une banque doit également joindre à sa demande de concession les curriculum vitae signés ainsi que les références des personnes chargées de l'administration et de la gestion. Etant donné que les banques sont également considérées comme intermédiaires financiers au sens de la LBA, une comparaison ne pouvait pas sans autre être exclue. Nous avons ensuite retenu que les documents demandés par l'OAR ne constituaient pas d'emblée une violation du principe de la proportionnalité. Nous avons rendu attentif l'intermédiaire financier au fait qu'il était libre de s'affilier à un autre OAR ou de se soumettre directement à l'autorité de contrôle.

Comme nous l'avons mentionné, la LBA n'est entrée en vigueur que le 1er avril 1998. Les intermédiaires financiers pouvaient en outre remettre une demande d'autorisation jusqu'au 1er avril 2000. C'est la raison pour laquelle il était encore trop tôt pour procéder à un examen complet des données personnelles demandées dans ce cadre. Nous avons cependant attiré l'attention de l'autorité de

contrôle en matière de lutte contre le blanchiment d'argent sur le fait qu'une nouvelle appréciation de la situation s'imposerait d'ici deux à trois ans. Celle-ci est nécessaire, notamment pour examiner quels documents sont vraiment nécessaires et appropriés pour atteindre le but poursuivi (lutte contre le blanchiment d'argent).

10. Publicité et marketing

10.1. Publicité non désirée et harcèlement de personnes faibles

Les campagnes de marketing agressives ayant pour cible des personnes âgées, voire malades sont de plus en plus fréquentes. Ces personnes affaiblies deviennent des proies faciles dans le cadre de la vente par correspondance. Par ailleurs, ces offensives publicitaires se doublent souvent d'un caractère international, ce qui complique la situation lorsque la victime souhaite se défendre.

Un réseau de commerce d'adresses dans le secteur de la voyance a ainsi vu le jour entre la Belgique et la Suisse. Les destinataires de prospectus sont généralement des personnes âgées vivants en Suisse ou en Belgique ayant eu recours, une fois ou l'autre, à un service ayant un rapport avec le domaine de la voyance. Le contenu des courriers provenant de Suisse et transitant pas Rotterdam est souvent fort semblable: les démarcheurs annoncent toutes sortes de prophéties heureuses et d'importants gains financiers si les personnes concernées acceptent de souscrire à l'offre proposée, mais leur font craindre l'arrivée d'évènements moins heureux si les personnes concernées déclinent leurs offres. Le tout bien sûr assorti de délais afin d' accentuer la pression pour obtenir des réponses.

Nos investigations nous ont permis de remonter la filière des démarcheurs. Suite à nos interventions, les plaignants ont reçu la confirmation que leurs données avaient été radiées des fichiers et n'ont, à notre connaissance, plus été importunés.

11. Statistiques

11.1. Les principes régissant le traitement des données personnelles à des fins statistiques

Les activités statistiques reposent également sur la collecte et le traitement de données personnelles. Ces données peuvent être source de convoitise et être d'une grande utilité pour l'ensemble des acteurs de la vie sociale, économique, culturelle, politique et administrative. Le risque existe que des données soient détournées et utilisées à des fins non statistiques. Les résultats statistiques anonymes et agrégés pourraient faire l'objet d'analyses ou de recoupements afin d'identifier les personnes formant la population observée.

Lorsque des organismes publics ou des entités privées collectent et traitent des données personnelles à des fins statistiques, ils sont tenus de prendre en compte les exigences de la protection des données afin de garantir à tout individu le respect de ses droits et libertés fondamentaux, notamment le droit au respect de la vie privée. En outre, les statisticiens se doivent, s'ils veulent pouvoir avoir accès aux données leur permettant de fournir des informations statistiques fiables, offrir des garanties élevées de confidentialité. La recherche d'un équilibre adéquat entre les exigences de la protection des données et les besoins en informations personnelles de la statistique est basée sur trois exigences fortes:

- transparence des traitements avec l'information des personnes concernées;

- respect strict du principe de finalité selon lequel les données collectées et traitées à des fins statistiques ne doivent pas être utilisées à d'autres fins;

- recours au traitement de données anonymes.

La confiance dans l'outil statistique est ainsi un préalable indispensable au bon fonctionnement et au développement de l'activité statistique. S'il subsiste un doute, même minime, sur l'utilisation des données collectées à des fins statistiques, cela aura des conséquences sur la confiance et la fiabilité de l'outil. Il est dès lors fondamental que le principe de finalité et le secret statistique soient garantis de manière absolue. Les données collectées et traitées à des fins statistiques ne doivent plus être utilisées à d'autres fins non statistiques se référant aux personnes concernées, notamment pour prendre des décisions ou des mesures à l'égard de ces personnes.

Dans cette optique, le fonctionnement et l'organisation de la statistique doivent évoluer. L'ère des grands recensements et des enquêtes exhaustives est vrai-

semblablement dépassée. On assistera de plus en plus à l'exploitation statistique de données qui ont été collectées et traitées pour d'autres finalités. Des enquêtes sectorielles sur la base d'échantillons de population (microrecensement) viendront dans certains cas compléter l'information. L'utilisation secondaire des données nécessite notamment une harmonisation des registres et des traitements pour permettre leur utilisation à des fins statistiques (une loi fédérale sur l'harmonisation des registres est en préparation). Cela entraînera de nouveaux défis pour le respect de la vie privée. Une telle harmonisation ne doit pas déboucher sur la création de nouveaux registres centralisés de population gérés par les organes statistiques. En effet, vu les pressions légitimées par la rationalisation et l'efficacité administratives, il est à craindre que de tels registres, comme cela est déjà le cas aujourd'hui pour les registres existants (registres des entreprises, registres des bâtiments et des logements) soient également utilisés à des fins non statistiques. Lorsqu'elles sont nécessaires pour certaines phases du traitement statistique, les données d'identification ne doivent plus être conservées de manière quasi permanente dans des registres statistiques. Ainsi, nous estimons que:

- la statistique doit s'orienter vers une diminution des traitements de données personnelles nécessitant la collecte, voire la conservation de données permettant d'identifier directement l'individu;

- en se basant sur les technologies de la vie privée, la statistique doit recourir à des données individuelles anonymes, notamment par l'utilisation de données d'identification codifiées ou par le recours à des pseudonymes.

Ces mécanismes permettent ainsi de limiter le traitement de données personnelles et assurent un meilleur respect des exigences de la protection des données dans le domaine de la statistique, notamment le principe de finalité. Ils ne restreignent pas l'accès aux informations, dont les statisticiens ont besoin, mais l'aménagent de manière différente.

11.2. Le droit de la protection des données dans les systèmes d'informations géographiques

Avec l'avènement de la société de l'information et l'explosion des technologies téléinformatiques, nous assistons à un profond bouleversement de notre environnement social et de nos manières d'appréhender l'information. De la qualité de l'information à disposition, de notre capacité et de nos possibilités d'accès aux informations pertinentes vont dépendre nos décisions individuelles, sociales, professionnelles, économiques, commerciales, politiques ou culturelles. Parmi les technologies de l'information actuellement en

expansion, les systèmes d'informations géographiques et les systèmes d'informations du territoire jouent un rôle important et font partie intégrante de l'infrastructure informationnelle.

Les systèmes d'informations du territoire sont des instruments de décision et de planification. Ils reposent sur des systèmes informatiques permettant la saisie et la gestion de données, ainsi que leur extraction standardisée ou spécifique. D'abord réservés à certains domaines d'activités de nos administrations publiques et notamment l'aménagement du territoire, le registre foncier, les mensurations cadastrales, la topographie, l'environnement ou la statistique, ces systèmes sont de plus en plus courtisés par d'autres entités publiques. Ils le sont également par le secteur privé, en particulier dans le domaine des assurances, du marketing, du renseignement de crédit, des transports ou du tourisme. On assiste ainsi à une multiplication des utilisations commerciales des systèmes d'informations géographiques et à une systématisation de la prise d'images digitalisées des bâtiments. Cela permet la mise en place de banques de données répertoriant l'ensemble des immeubles. En outre, ces informations sont de plus en plus destinées à être mises à la disposition du grand public.

Si de nombreuses applications en relation avec les systèmes d'informations géographiques sont légitimes et répondent à un intérêt public non contesté, l'impact technologique et informationnel de ces systèmes, confèrent à leurs concepteurs et à leurs utilisateurs une lourde responsabilité sociale. Ces systèmes revêtent de nombreux aspects positifs. Ils comportent également des aspects négatifs qu'il convient de maîtriser. L'un de ces effets négatifs a trait aux atteintes réelles ou potentielles aux droits de la personnalité et aux droits et libertés fondamentaux, notamment le droit à la vie privée des personnes.

En abordant le problème des systèmes d'informations géographiques, nous avons au premier abord l'impression que ces systèmes ne touchent pas la protection des données personnelles. Un système d'informations géographiques est d'abord lié au territoire, à l'espace et à l'environnement. Il ne devrait en soi pas contenir d'informations liées à une personne déterminée, identifiée ou identifiable. Toutefois, les données spatiales ne comprennent pas seulement des données purement géographiques. Elles contiennent également des données dites attributaires, statistiques, économiques qui peuvent avoir un caractère personnel, c'est-à-dire se référant à une personne identifiée ou identifiable. Les systèmes d'informations géographiques, en recourant à l'utilisation de banques de données relationnelles, permettent la saisie à la fois des données géométriques (données géocodées, positions, coordonnées) et des données de fait (caractéristiques, attributs). Ils facilitent la liaison de ces données dans un rapport complexe et logique tant au niveau du contenu que de l'espace. Les technologies informatiques permettent en effet à la cartographie d'évoluer vers des modèles

complexes qui offrent des analyses très précises et qui facilitent de ce fait l'identification des personnes. Les systèmes d'informations géographiques couplés aux techniques de télédétection, notamment par satellites, rend ainsi aisé le repérage sur une carte de phénomènes qui sont difficilement relevables par une observation sur place. Il est ainsi possible d'identifier des personnes en relation avec un lieu, un objet ou un immeuble. Grâce à ces techniques, il est par exemple possible de repérer un véhicule, de localiser un immeuble, de surveiller l'utilisation de subventions agricoles ou de contribuer au contrôle de sinistres. Ces systèmes sont ainsi des outils très performants permettant l'intégration des données, en particulier en les connectant à leur localisation géographique (procédure de géocodage). Dans des secteurs comme le marketing, les assurances ou les renseignements de crédits, cette technique s'avère très prometteuse et offre des possibilités insoupçonnées d'assemblage et de compilation des données à partir de différentes sources d'informations qui touchent les individus, les ménages ou les entreprises. En effet, il est possible de coupler des informations provenant de sources différentes et notamment de registres publics et de les rendre accessibles à différents utilisateurs. Des cartes peuvent être élaborées de manière à faire apparaître à l'échelon d'une petite commune, d'un quartier ou d'une rue, le profil des ménages selon l'âge, la profession, le nombre d'enfants, le niveau des revenus ou de la fortune, le type d'habitat etc. Les systèmes d'informations géographiques sont devenus des instruments performants dans l'analyse et le traitement de données à caractère personnel. Grâce à leur puissance d'intégration des données et à leur capacité d'analyse, grâce au caractère local ou spatial des données, de tels systèmes ont un potentiel d'intrusion dans la vie privée que d'autres systèmes d'informations ne connaissent pas.

Le développement des systèmes d'informations géographiques et des systèmes d'informations du territoire doivent tenir compte des exigences d'un Etat de droit dans une société démocratique. Ils doivent en particulier respecter la personnalité et les droits fondamentaux. Il est dès lors nécessaire d'entourer la mise en place de tels systèmes et leur utilisation d'un environnement légal et réglementaire approprié assurant la protection des données tout en tenant compte des intérêts publics ou privés prépondérants pouvant légitimer le traitement de données personnelles. En particulier, il est important de garantir:

- La transparence des traitements de données personnelles dans un système d'informations géographiques. A cet effet, les personnes concernées doivent être informées sur les finalités du système, les catégories de données traitées, les utilisateurs du système et les destinataires des informations et pouvoir faire valoir leurs droits.

- Les finalités du système d'informations géographiques doivent être déterminées et respectées. En particulier, si les finalités du système ne se rapportent pas aux personnes concernées, notamment dans le cadre d'activités statisti-

ques, il faut veiller au respect du secret statistique et garantir l'anonymat lors de la publication ou de la diffusion.

- Le catalogue des données traitées doit être établi et seules les données nécessaires au but du traitement doivent être collectées et traitées.

- La qualité des données doit être garantie (exactitude, mise à jour, conservation limitée dans le temps).

- Les communications de données et en particulier par procédure d'appel doivent être clairement réglées.

- Le cadre juridique doit également être accompagné de mesures techniques et organisationnelles. Il conviendrait en particulier d'encourager le développement et le recours à des technologies dites de la vie privée.

- Les droits des personnes concernées doivent être garantis. En particulier, le droit à l'information préalable, le droit d'accès aux données qui les concernent et notamment le droit de s'opposer à la collecte systématique et au traitement à des fins commerciales des données sous forme d'images de leur environnement d'habitation. La personne concernée doit notamment pouvoir s'opposer à ce que ses données soient diffusées sur Internet ou enregistrées sur un CD-Rom.

11.3. Mise en œuvre du recensement de la population 2000

Dans le cadre du recensement 2000, le jour "J" était fixé au 5 décembre 2000. Toutes les personnes résidant en Suisse à cette date ont eu l'obligation de remplir leurs questionnaires, afin de contribuer à cette vaste statistique visant à établir une photographie socioculturelle du pays. Notre tâche a été de veiller à ce que les dispositions fédérales relatives à la protection des données soient observées. De manière générale, les différentes opérations du recensement 2000 se sont déroulées correctement. Il convient cependant de rester vigilant et de poursuivre notre travail de conseil et de contrôle.

Le 5 décembre 2000 a eu lieu le recensement de la population 2000. La phase de préimpression des questionnaires individuels et de ménage ainsi que des bordereaux de logement étant achevée, les personnes résidentes en Suisse les ont reçus. Les cantons de Lucerne et du Jura ont rencontré quelques difficultés liées aux données préimprimées. Les autorités cantonales de surveillance y ont

remédié et les erreurs ont pu être rectifiées. Les questionnaires remplis ont ensuite été transmis au centre de services pour traitement, soit par courrier, soit par Internet par le biais du système «e-census». Les données du recensement par Internet ont été transmises grâce à un cryptage de 128 bits qui correspond au standard technique d'aujourd'hui et garantit une grande sécurité. Le concept, baptisé «e-census», a été élaboré par l'Office fédéral de la statistique (OFS) et fait l'objet d'une attention particulière de notre part. Un règlement de traitement nous a été soumis. Il sera très utile dans le cadre de notre tâche de contrôle.

La grande majorité des cantons et de nombreuses communes ont confié à un centre de services des tâches relatives au recensement. Ce dernier, mandaté par l'OFS, réunit diverses entreprises. Leurs locaux sont situés dans plusieurs villes et cantons.

Le processus concernant le traitement des questionnaires peut être résumé comme suit. A leur arrivée, les questionnaires remplis à la main ont été scannés au centre de tri postal à Lucerne. Leur version électronique a ensuite été transmise à l’entreprise DCL Data Care AG à Kriens (canton de Lucerne). Là, la version électronique de l'ensemble des questionnaires a été améliorée sur le plan de la lisibilité.

Un service de renseignement téléphonique (hot-line) a été chargé de répondre aux questions des personnes qui devaient remplir les formulaires.

Après la date fixée pour la reddition des questionnaires, soit le 12 décembre 2000, un concept de rappels écrits et téléphoniques a été mis en œuvre.

Le centre de services a été obligé de prendre toutes les mesures nécessaires pour garantir la protection des données. En particulier, DCL a dû s'en tenir aux exigences de protection des données définies dans la loi fédérale sur le recensement, son ordonnance d'application, dans les directives de l'OFS relatives aux travaux du centre de services, ainsi que dans le contrat qu'elle a conclu avec l’OFS.

L'Unité de stratégie informatique de la Confédération, ainsi que nos représentants ont contrôlé le système informatique du centre de services avant sa mise en fonction. Par ailleurs, un organe de contrôle extérieur a été engagé et a élaboré un rapport sur la protection des données au centre de services.

En mai 2000, un groupe de contrôle chargé de la protection des données et composé de représentants cantonaux (Zürich, Bâle-Campagne et Fribourg) et de nous-même a été formé. Ce groupe a été actif pendant la phase de pré-impression des formulaires du recensement. En tant qu'organe de surveillance, il a

veillé à ce que les instructions concernant la protection des données soient respectées et coordonnées sur le plan cantonal et fédéral.

Les cantons membres du groupe de contrôle ont proposé de suspendre leur participation à partir du 5 décembre 2000, car cette date correspondait au début d'une nouvelle phase, laquelle concerne avant tout des tâches fédérales, relevant de notre compétence. Les responsables dans les cantons se sont dès lors concentrés sur le traitement des données dans les cantons et les communes. Ils conservent cependant la possibilité de procéder à des contrôles auprès du centre de services en ce qui concerne le traitement des données que les cantons et les communes ont délégués à DCL.

En ce qui nous concerne, nous avons effectué plusieurs contrôles entre décembre 2000 et janvier 2001 auprès des différents postes chargés d'effectuer des tâches en rapport avec le recensement 2000. Nos représentants ont ainsi visité:
- les bâtiments du centre de tri postal (la Poste suisse) à Lucerne où étaient réceptionnées les enveloppes contenant les questionnaires;
- le centre de services DCL à Kriens;
- la hot-line et
- le call-center chargé de compléter les questionnaires.

Ces visites ont eu pour objectif l'examen du respect des dispositions relative à la protection des données. Les locaux ont été inspectés afin de s'assurer que la sécurité concernant l'accès et la conservation des données était garantie. Les employés ont été questionnés, afin de s'assurer du fait qu'ils avaient été formés et sensibilisés aux questions relevant de la protection des données. Les moyens de communication, ainsi que les supports de données ont été examinés. Enfin, la sécurité informatique a été contrôlée.

Ces contrôles n'ont pas donné motif à craindre pour la sécurité des données. Les documents nécessaires au contrôle ont été mis à disposition et les tests ponctuels ciblés ont permis de constater que les tâches sont accomplies correctement, par un personnel informé du secret de fonction en vigueur.

Le recensement se poursuivra avec le relevé des données manquantes (travail de complétude), l'enquête de couverture, le retour des données dans les cantons et les communes, l'anonymisation, l'évaluation des données figurants dans les questionnaires retournés et enfin avec la destruction ou l'archivage des divers supports ayant servi au recensement 2000. Nous procéderons au contrôle de chacune de ces prochaines étapes.

12. Modernisation de la protection des données

12.1. Vers une modernisation de la protection des données

Suite à l'adoption de deux motions de la Commission de gestion et de la Commission des affaires juridiques du Conseil des Etats, l'Office fédéral de la justice a été chargé de préparer un avant-projet de révision de la loi fédérale sur la protection des données. Cet avant-projet sera soumis en procédure de consultation en 2001. Le préposé fédéral à la protection des données participe aux travaux.

Huit années après son entrée en vigueur, le Conseil fédéral s'apprête à soumettre au parlement un message en vue d'une modification partielle de la loi fédérale sur la protection des données (LPD). Cette modification doit permettre de donner suite à la motion 98.3529 de la Commission de gestion du Conseil des Etats «Liaisons on-line: Renforcer la protection pour les données personnelles» et à la motion 00.3000 de la Commission des affaires juridiques du Conseil des Etats «Renforcement de la transparence lors de la collecte des données personnelles». Aux termes de ces deux motions, la révision portera tout d'abord sur la mise en place d'une base légale permettant de mener des projets pilotes avec des accès par procédure d'appel. Elle fixera des normes minimales régissant notamment l'accès, l'utilisation et le contrôle des banques de données fédérales afin d'améliorer la collaboration entre la Confédération et les cantons. Enfin, elle introduira le devoir d'informer les personnes concernées lors de la collecte de données personnelles sensibles ou de profils de la personnalité. La révision devrait également porter sur d'autres aspects.

L'opportunité d'une révision doit nous amener à tirer un bilan de l'application de la LPD et d'examiner dans quelle mesure la loi mérite d'être modifiée. Bien que relativement récente, la LPD repose sur le concept des législations de protection des données de la fin des années 70. Toutefois à la différence de certaines lois étrangères ou cantonales, elle suit une approche non technologique qui offre une certaine souplesse et permet une meilleure adaptation à l'évolution technologique. Une modernisation de la protection des données, notamment pour tenir compte de l'évolution du droit européen, de l'évolution des technologies de l'information, de la globalisation et de la dissémination des échanges d'informations est néanmoins souhaitable. Dans ce cadre, il conviendrait de:

- mettre à jour le catalogue des définitions, notamment pour tenir compte des évolutions technologiques;
- de revoir le système de déclaration des flux transfrontières de données qui n'est pas adapté à la réalité des transactions internationales, notamment par Internet;

- de revoir le registre des fichiers qui s'avère un instrument lourd quant à sa gestion et dont l'efficacité est limitée;
- de renforcer la position de la personne concernée qui se trouve dans une position délicate face à la non-transparence des traitements et aux moyens de défense dont elle dispose en particulier dans le secteur privé;
- de renforcer les compétences du préposé fédéral lesquelles pourraient être élargies;
- d'aplanir la différence du niveau de protection entre le secteur public et le secteur privé. Une telle différence n'est plus justifiée, notamment eu égard à la politique de privatisation qui s'est amorcée depuis quelques années. Les conditions de traitement des données sensibles et des profils de la personnalité dans le secteur privé doivent ainsi être renforcées.
- d'examiner l'articulation avec le projet de loi fédérale sur la transparence de l'administration et notamment l'opportunité de rassembler les deux lois (voir 7ème rapport d'activités 1999/2000, pages 203ss).

La modification devrait également provoquer une processus de révision dans les cantons dotés d'une loi et inciter les cantons qui n'ont toujours pas adopté de loi à le faire. Il convient en effet d'assurer l'harmonisation entre le droit fédéral et le droit cantonal et éventuellement de revoir la répartition des compétences entre Confédération et cantons, notamment lorsque des traitements sont effectués par les cantons en application du droit fédéral.

Ainsi, la présente révision ne devrait pas se limiter à la réalisation des deux motions. Toutefois, une modernisation de la protection des données ne doit pas déboucher sur une révision totale de la LPD et ne doit pas remettre en cause les principes fondamentaux de la protection des données, tels qu'ils découlent de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). La structure de la loi doit également être maintenue. Les objectifs d'une modernisation de la protection des données sont les suivants:

- Le renforcement de la position et de la responsabilité de l'individu face au traitement de données personnelles qui le concernent. La garantie du droit de l'individu à l'autodétermination en matière d'information implique que celui-ci soit en mesure de participer activement au développement de la société de l'information et d'assumer sa responsabilité par rapport aux traitements qui le concernent. Il doit ainsi bénéficier du droit d'être informé sur les traitements qui le concernent et cela avant que les données ne soient collectées ou communiquées. Il doit pouvoir s'opposer sans entraves excessives au traitement de données qu'il ne souhaite pas et qu'il n'est pas obligé d'accepter. Il doit pouvoir disposer de moyens (notamment techniques) de gérer la protection de sa vie privée et de déterminer quelles données personnelles le concernant peuvent être traitées et par qui. A cette fin, la loi doit

promouvoir le recours à des mécanismes permettant de crypter les données, de communiquer de manière anonyme ou d'utiliser des pseudonymes.

- Le renforcement de la responsabilité des personnes et des organes qui traitent ou font traiter des données personnelles. Les responsables de traitement doivent ainsi assurer une meilleure transparence des traitements qu'ils effectuent. Ils doivent avoir l'obligation d'informer les personnes concernées lors de la collecte de données. Contrairement à la motion de la Commission des affaires juridiques du Conseil des Etats, ce devoir d'information ne doit pas être limité aux données sensibles ou aux profils de la personnalité, mais couvrir tout traitement de données quelle que soit la nature des données. En effet, nous avons pu le constater, nombreux sont les traitements ne portant pas sur des données sensibles et effectués à l'insu des personnes concernées. Ils entraînent des atteintes à la personnalité dont les conséquences peuvent être graves pour la personne, sans qu'elle ait la possibilité de faire valoir ses droits. C'est particulièrement vrai dans le secteur financier. Les responsables de traitement doivent également gérer leurs traitements de données de manière plus transparente et documentée. Ainsi, la loi devrait les inciter à procéder régulièrement à des révisions (audit) de protection des données et favoriser la création de labels de protection des données. Elle devrait également prévoir la possibilité pour les organisations professionnelles et associations faîtières d'élaborer des codes de conduite en matière de protection des données, complétant et concrétisant les exigences légales.

- L'incitation au recours aux technologies qui permettent de garantir le respect de la vie privée afin que les systèmes de traitement des données personnelles (matériel et logiciel) tiennent compte des exigences de la protection des données dès leur conception et lors de leur développement. Ils doivent être élaborés selon le principe d'un emploi économe des données. A cette fin, la loi doit permettre et encourager le recours à des techniques d'anonymisation des données et de pseudonymisation chaque fois que cela est possible et n'est pas disproportionné par rapport aux risques d'atteinte à la vie privée.

- L'harmonisation de la législation suisse avec le droit européen dans la mesure où cela est nécessaire notamment pour éviter aux responsables de traitement, dont les activités de traitement des données se déroulent également au sein de l'Union européenne d'être confrontés à des exigences différentes en matière de protection des données.

- La réalisation du protocole additionnel à la Convention 108 qui prévoit l'obligation des Parties d'instituer une ou plusieurs autorités de contrôle indépendantes. Il règle également les communications transfrontières de données vers des destinataires situés dans des Etats n'ayant pas ratifié la

Convention (voir 7ème rapport d'activités 1999/2000, pages 219 et ci-après page 213).

- La diminution des contraintes bureaucratiques de la loi en renonçant à des obligations de déclaration lorsqu'elles n'apportent rien du point de vue de la protection des données. Ainsi, la déclaration des flux transfrontières de données pourrait être abandonnée. Le registre des fichiers qui doit jouer un rôle quant à la transparence des traitements doit être modifié. Les responsables de traitement pourraient être tenus de gérer la liste des traitements qu'ils opèrent et de la tenir accessible à tout un chacun. Le registre des fichiers géré par le PFPD pourrait se limiter aux traitements portant sur des données sensibles et des profils de la personnalité ou qui impliquent des communications régulières de données.

- Le renforcement du contrôle de la protection des données. La loi devrait institutionnaliser les conseillers à la protection des données auprès des organes fédéraux et des personnes privées responsables de traitement et leur confier des tâches de contrôle.

- Le renforcement des compétences de conseil et de médiation du préposé fédéral à la protection des données. La médiation entre le responsable du traitement et les personnes concernées est un instrument adéquat pour permettre aux individus de faire valoir leurs droits sans recourir à des procédures civiles ou administratives qui peuvent s'avérer fastidieuses et coûteuses. Dans le secteur privé en particulier, l'individu hésite à engager une procédure dans laquelle il est souvent en position de faiblesse par rapport aux moyens de défense du responsable du traitement. Le préposé fédéral devra à l'avenir axer son action principalement sur les activités de conseil, de médiation, de formation et d'information. Il devra être en mesure d'anticiper les développements technologiques et de fournir des conseils sur la manière de développer des systèmes de traitement conformes aux exigences de la protection des données. Des contrôles demeureront néanmoins nécessaires et devront être entrepris essentiellement dans les situations où le traitement est susceptible de porter une atteinte grave à un grand nombre de personnes. Dans cette optique, le préposé doit disposer de compétences d'investigation renforcées. A l'instar des compétences qui sont accordées au Contrôle fédéral des finances, il conviendrait d'examiner la possibilité pour le préposé de procéder à des traitements et notamment d'interroger des banques de données pour vérifier leur conformité à la loi. Il doit également avoir le moyen de faire respecter ses recommandations. En particulier, il doit pouvoir porter ses recommandations adressées aux organes fédéraux devant la Commission fédérale de la protection des données (voir 6ème rapport d'activités 1998/99, pages 323ss et 372ss).

II. AUTRES THÈMES

1. Droit d'accès

1.1. Droit d'accès auprès des organes fédéraux

Le droit d'accès est un droit fondamental pour la personne concernée et l'institution-clé de la protection des données. C'est l'unique moyen pour l'intéressé de faire valoir ses droits. Un organe fédéral doit, sauf disposition légale contraire, appliquer la loi fédérale sur la protection des données en matière de droit d'accès. En cas de refus ou de limitation de ce droit, l'organe fédéral doit rendre une décision motivée.

Une personne a demandé à un office fédéral l'accès à tous les documents le concernant. L'office en question a communiqué au requérant une partie des pièces souhaitées en procédant sur certains documents à des caviardages sans en indiquer les motifs. Le demandeur s'est adressé par la suite au département compétent en invoquant la violation de la loi fédérale sur la protection des données (LPD), en particulier les dispositions relatives au droit d'accès. Il s'est également adressé quelques jours plus tard au Préposé fédéral pour exposer son cas et demander si la pratique de l'office était conforme à la LPD. Dans les cas ou le droit d'accès est limité, l'organe fédéral maître du fichier doit informer l'intéressé par écrit sous forme de décision motivée dans les 30 jours suivant réception de la demande. Nous avons donc prié l'office de régler le cas conformément à la LPD. Cette démarche est restée vaine. De plus le département compétent a répondu au requérant que la LPD n'était pas applicable dans le cas d'espèce pour la simple raison qu'il n'existait pas de fichier. Par fichier on entend tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée. La communication au requérant de documents le concernant démontre clairement l'existence d'un fichier et par conséquent l'application de la LPD. Nous sommes intervenus une nouvelle fois auprès du département pour lui rappeler que la LPD était applicable. Finalement le demandeur a obtenu de l'office une décision conforme au droit applicable et, le cas échéant, il pourra faire usage des voies de recours en la matière.

L'organe fédéral maître de fichier doit communiquer au requérant non seulement toutes les données le concernant qui sont contenues dans le fichier, mais également le but du traitement, éventuellement sa base juridique, les catégories de données personnelles traitées, les participants au fichier ainsi que les destinataires des données. L'organe fédéral peut refuser ou restreindre la communication des renseignements si une loi le prévoit comme c'est le cas des banques de données en matière de lutte contre la criminalité où le législateur a prévu un

mécanisme de droit d'accès indirect exercé par le préposé fédéral. Le maître de fichier peut également invoquer un intérêt prépondérant d'un tiers, par exemple la présence sur le document communiqué de données concernant la santé d'une tierce personne. Un intérêt prépondérant public peut également être invoqué comme la sûreté intérieure ou extérieure de la Confédération. Le risque de compromettre le déroulement d'une procédure d'instruction en cours peut également motiver un refus ou une restriction du droit d'accès. Comme nous l'avons indiqué ci-dessus, le refus ou la limitation du droit d'accès doit faire l'objet d'une décision motivée. Le demandeur peut recourir auprès du département et la décision de ce dernier peut être portée devant la Commission fédérale de la protection des données. Les décisions de cette commission peuvent faire l'objet d'un recours de droit administratif devant le Tribunal fédéral.

1.2. Refus de consulter les notes de l'examinateur

Les notes prises pour l'usage personnel ne tombent en principe pas sous le coup de la loi sur la protection des données. Néanmoins, cette règle n'est pas toujours valable: un candidat à un examen a le droit de pouvoir consulter les notes que les examinateurs ont prises durant l'examen oral.

Après l'annonce de son échec à l'examen du diplôme fédéral de chef de vente, un candidat malchanceux désire consulter son dossier d'examen. On lui répond qu'il ne peut accéder qu'aux documents de l'examen écrit. La commission d'examen, un organe fédéral au sens de la loi fédérale sur la protection des données, lui refuse en effet l'accès aux notes prises par les examinateurs durant les examens oraux. La commission d'examen s'appuie pour cela sur des instructions émanant de l'Office fédéral de la formation professionnelle et de la technologie, lesquelles excluent même expressément le droit de consulter les notes personnelles des experts.

La loi fédérale sur la protection des données n'est en principe pas applicable aux données personnelles qui sont traitées par une personne physique dans un but exclusivement personnel et ne sont pas communiquées à des tiers. Ce principe est applicable aux notes destinées à la sphère privée comme aux notes établies dans l'exercice d'une profession, qui ne servent que d'aide-mémoire ou de base de travail. Il en va toutefois autrement des notes que les examinateurs ont prises durant les examens oraux.

En effet, il est rare que les notes des examinateurs servent uniquement à l'usage personnel. Par exemple, on ne peut plus parler d'usage personnel lorsque l'examinateur cite publiquement à l'occasion des délibérés le contenu des notes qu'il

a prises ou dépose comme il le doit ses notes dans le dossier d'un candidat, dossier qu'une tierce personne peut consulter. En outre, ces notes sont déterminantes pour l'attribution ultérieure du résultat d'examen et représentent davantage qu'un aide-mémoire de l'examinateur. Les notes prises au cours d'un examen par l'examinateur tombent donc clairement dans le domaine d'application de la loi sur la protection des données.

La commission d'examen ne peut pas davantage s'appuyer sur l'argument selon lequel ces notes constituent un document interne pour en refuser l'accès. Les documents internes sont ceux qui servent uniquement à la formation d'une opinion au niveau administratif interne et ne peuvent donc pas être dévoilés au public. Or le droit d'accès prévu par la loi sur la protection des données - contrairement au droit d'accès en droit procédural - englobe aussi les documents internes.

En s'appuyant sur le droit d'accès prévu par la loi sur la protection des données, le candidat peut demander que toutes les données le concernant dans le dossier d'examen lui soient communiquées, donc aussi les notes prises par les examinateurs. Les exceptions au droit d'accès sont citées de manière exhaustive dans la loi sur la protection des données. Ainsi le maître du fichier ne peut refuser, restreindre les renseignements demandés, voire en différer l'octroi que lorsqu'une loi au sens formel le prévoit ou lorsqu'un intérêt prépondérant d'un tiers l'exige. Un organe fédéral, comme dans le cas présent la commission d'examen, peut en outre refuser, restreindre ou différer l'octroi du renseignement demandé lorsqu'un intérêt public prépondérant, en particulier la sûreté intérieure ou extérieure de la Confédération l'exige ou encore lorsque l'octroi des renseignements risque de compromettre une instruction pénale ou une autre procédure d'instruction.

Nous sommes donc d'avis qu'un candidat doit avoir le droit de consulter tous les documents d'examen le concernant, y compris les notes établies par les examinateurs.

2. Carte-client

2.1. Carte clients: carte M-Cumulus

La Migros n'est pas autorisée à communiquer à une commune l'identité d'une personne, titulaire dune carte M-Cumulus, soupçonnée de contrevenir à un règlement administratif relatif à l'entreposage des poubelles.

Dans notre 7ème rapport d'activités 1999/2000 (pages 194-195), la question de savoir si la Migros était autorisée ou non à communiquer à un juge d'instruction les coordonnées d'une personne titulaire d'une carte M-Cumulus, avait été traitée. Un ticket de caisse avec numéro M-Cumulus avait été retrouvé dans une poubelle. Le thème avait alors été examiné sous l'angle du droit de refuser de témoigner. La réponse avait été affirmative puisque la Migros ne figurait pas au nombre des personnes exemptées de par la loi à témoigner en justice. Le juge d'instruction qui avait requis cette mesure avait pu obtenir l'identité du titulaire de la carte dans le cadre d'une procédure pénale pendante.

Au cours de l'année 2000, nous avons traité un cas différent: la Migros souhaitait savoir si une demande de renseignement, émanant cette fois-ci d'une commune, pouvait être satisfaite. Cette dernière agissait en qualité d'organe d'application d'un règlement administratif communal relatif à la gestion des poubelles.

Notre réponse a été négative. La transmission d'une information de ce type, dans le cadre d'une procédure administrative de première instance, est soumise à la loi fédérale sur la protection des données. Une telle communication déroge au principe de finalité qui est à la base de la collecte des données d'identification liée à la carte M-Cumulus. Il n'est pas inutile de rappeler que la Migros s'engage à ne traiter les données qu'au sein de la coopérative Migros à des fins de statistiques ou de marketing et à ne pas les transmettre à des tiers extérieurs.

3. Vidéosurveillance

3.1. Surveillance par vidéo dans le secteur privé - exigences minimales de la protection des données

Les personnes privées ne sont autorisées à recourir à des systèmes de surveillance par vidéo que si les principes généraux de la protection des données sont respectés. Suite au nombre élevé de demandes qu'il a reçu à ce sujet, le PFPD a édité un aide-mémoire sur ce thème.

On constate une utilisation de plus en plus fréquente dans le secteur privé de systèmes de surveillance par vidéo dans le but de protéger des personnes ou d'éviter des déprédations. Ceci explique que nous avons reçu plusieurs demandes à ce sujet. C'est pourquoi nous avons rédigé un aide-mémoire qui résume les conditions générales qui doivent être remplies pour mettre en œuvre un système de surveillance par vidéo (voir page 240). Celui-ci ne couvre cependant pas le domaine de la surveillance par vidéo sur le lieu de travail.

L'utilisation de caméras vidéo par des personnes privées à des fins de surveillance est soumis à la loi fédérale sur la protection des données dans la mesure où les images filmées concernent une ou plusieurs personnes identifiées ou identifiables, ceci indépendamment du fait que les images soient conservées ou non. Les traitements effectués (prise de vue, communication, visionnement immédiat ou subséquent, conservation des images etc.) doivent être en conformité avec les principes généraux de la protection des données.

Un système de surveillance par vidéo ne peut être utilisé que si les deux conditions suivantes sont remplies:

- La surveillance par vidéo ne peut être utilisée que si l'atteinte à la personnalité qu'elle constitue est justifiée par le consentement de la personne concernée, par un intérêt prépondérant privé ou public ou par la loi. Ainsi, un bijoutier peut avoir un intérêt prépondérant à ce que son commerce ne soit pas cambriolé pendant son absence (principe de la licéité).
- La surveillance par vidéo doit constituer un moyen approprié et nécessaire pour atteindre le but recherché, à savoir assurer la sécurité, en particulier la protection de personnes et/ou de biens. Elle ne peut être utilisée que si d'autres mesures entravant moins la vie privée, telles que des serrures supplémentaires, un renforcement des portes d'entrée, des systèmes d'alarme se sont révélées insuffisantes ou irréalisables. Ainsi, l'installation de caméras vidéo dans une halle d'entreposage pour éviter des actes de vandalisme sera en règle générale admissible (principe de la proportionnalité).

Les règles suivantes doivent être respectées lors de l'installation et de l'exploitation d'un système de surveillance par vidéo:

- La personne responsable du système de surveillance par vidéo doit informer les personnes qui pénètrent dans le champ de prise de vue de la présence d'un tel système à l'aide d'un panneau indicateur bien visible. Si les images prises sont liées avec un fichier, ce panneau doit en outre indiquer auprès de qui on peut faire valoir son droit d'accès, pour autant que cela ne ressorte pas clairement des circonstances. Ainsi, une caméra vidéo placée à l'entrée d'un immeuble locatif devra être signalée par un panneau bien visible pour

toute personne qui pénètre dans le bâtiment (principe de la bonne foi et droit d'accès).

- La personne responsable du système de surveillance par vidéo doit prendre les mesures techniques et organisationnelles nécessaires pour éviter tout traitement non autorisé des données personnelles (par ex. en interdisant l'accès aux données aux personnes non autorisées). Ainsi, seules les personnes autorisées ont accès aux écrans des caméras vidéo. D'autre part, les données enregistrées doivent être conservées en un endroit sûr, par ex. dans un local fermé à clé et seulement les personnes autorisées doivent avoir accès à la clé (sécurité des données).
- La caméra vidéo doit en outre être placée de telle manière que son champ de vision soit limité de façon à ce que seules les prises de vue absolument nécessaires pour atteindre le but fixé soient prises. Ainsi, une caméra placée à l'entrée d'un immeuble locatif ne devra en principe pas permettre de voir quelle personne se rend dans quel appartement ou en ressort (principe de la proportionnalité).
- Les données doivent être utilisées uniquement pour protéger des personnes et des biens. Elles ne peuvent pas être utilisées à d'autres fins. Ainsi, les images prises par une caméra vidéo installée dans le but d'assurer la sécurité ne pourront pas être utilisées à des fins de marketing (principe de la finalité).
- Les données personnelles enregistrées par une caméra ne doivent pas être communiquées, à l'exception des cas prévus ou autorisés par la loi, par ex. une demande émanant d'un juge. Les images prises ne peuvent pas non plus être transmises à des tiers à des fins de marketing (principe de la finalité).
- Les images prises par la caméra doivent être effacées aussi rapidement que possible. En règle générale, les déprédations ou les agressions sont découvertes quelques heures après qu'elles aient été commises. Cela signifie qu'au vu du but poursuivi une durée de conservation de 24 heures est suffisante si aucune déprédation ou dommage corporel n'a été découvert pendant ce laps de temps. Pour les surveillances par vidéo effectuées dans des locaux privés qui ne sont pas accessibles au public, ce délai peut dans certains cas être plus long. Ainsi, une absence pour cause de vacances peut justifier une durée de conservation plus longue. Mais même dans ce cas, les images devront être détruites aussi vite que possible après le retour si aucune déprédation n'a été constatée (principe de la proportionnalité).

Vous trouverez également des informations sur la vidéosurveillance sur page 212

3.2. Surveillance par vidéo dans les transports publics - exigences minimales de la protection des données

Les transports publics recourent plus souvent aux caméras vidéo, d'une part pour combattre le vandalisme, d'autre part pour procurer un meilleur sentiment de sécurité. Si une surveillance par caméra vidéo est effectuée, elle doit être visible pour les passagers. D'autre part, les images doivent en règle générale être détruites après 24 heures. Si l'entreprise de transport est un organe fédéral, elle a en outre besoin d'une base légale pour justifier sa surveillance par vidéo.

On remarque une tendance au sein des transports publics à utiliser des systèmes de surveillance par vidéo pour combattre le vandalisme et pour assurer la sécurité des personnes. C'est ainsi que les Chemins de fer fédéraux (CFF) nous ont soumis leur projet qui prévoit d'équiper les trains régionaux non accompagnés de caméras vidéo.

Les entreprises de transport soumises au droit privé doivent en principe remplir les mêmes conditions pour la surveillance par vidéo que celles qui valent pour le secteur privé (voir nos explications aux pages 189 sur la surveillance par vidéo dans le secteur privé). Si la surveillance par vidéo est effectuée par une entreprise de transport qui est considérée comme organe fédéral au sens de la protection des données, celle-ci nécessite en plus une base légale.

Dans les transports publics, une surveillance par vidéo ne peut par principe être effectuée que pour augmenter la sécurité des passagers ainsi que pour combattre le vandalisme. D'autre part, cette surveillance par vidéo dans les transports publics doit être nécessaire et apte à atteindre le but poursuivi. Elle n'est pas admissible si le but peut être atteint par des mesures moins radicales. D'autre part, les personnes concernées doivent être rendues attentives à la surveillance par vidéo à l'aide de panneaux placés de manière bien visible, par ex. près des portes d'accès. Si les images prises sont liées avec un fichier, ce panneau doit en outre indiquer auprès de qui on peut faire valoir son droit d'accès, pour autant que cela ne ressorte pas clairement des circonstances. Les mesures techniques et organisationnelles appropriées doivent être prises pour protéger les données enregistrées contre un accès par des personnes non autorisées. La caméra vidéo doit en outre être placée de telle manière que son champ de vision soit limité de façon à ce que seules les prises de vue absolument nécessaires pour atteindre le but fixé soient prises. Les prises de vue doivent être utilisées uniquement pour le but poursuivi. D'autre part, les images qui ne sont pas liées à un incident doivent être détruites au plus tard après 24 heures.

Dans la mesure où toutes ces conditions sont remplies, il est admissible du point de vue de la loi sur la protection des données d'utiliser des systèmes de surveillance par vidéo.

4. Publication de données personnelles

4.1. Publication de comptes en déshérence

Au cours des années précédentes, nous avons eu l'occasion de nous exprimer à plusieurs reprises sur les fonds en déshérence datant de la Seconde guerre mondiale (se reporter à ce propos au 5ème rapport d'activités 1997/98, page 212 et au 6ème rapport d'activités 1998/99, page 313). Par ailleurs, nous avons abordé plus en détail dans le dernier rapport d'activités les modalités d'accès à une liste publiée sur Internet qui contenait des données concernant quelque 26'000 comptes.

Sur la base des recommandations de l'«Independent Committee of Eminent Persons», la Commission fédérale des banques décida que les banques suisses devaient publier une liste des comptes en déshérence encore ouverts ainsi que de certains comptes clos ayant un lien probable avec des victimes de l'Holocauste. L'Association suisse des banquiers avait donc l'intention de publier la liste de quelque 26'000 comptes sur Internet. Le nom, le prénom, le pays de domicile du titulaire du compte, ainsi qu'une indication sur l'état du compte et le montant déposé auraient dû être publiés. L'Association suisse des banquiers a consulté le PFPD pour savoir quels étaient les principes du droit de la protection des données qu'il convenait de respecter à cet égard. Les services américains mandatés demandaient que la liste entière comprenant les 26'000 comptes soit publiée sur Internet et qu'elle puisse être copiée afin de permettre aux personnes concernées d'y accéder le plus facilement possible.

Les principes généraux du droit de la protection des données sont également applicables aux publications sur Internet. La publication d'une liste rassemblant 26'000 comptes en déshérence se heurte à un principe majeur de la protection des données, celui de la proportionnalité. D'après ce principe, une consultation sur Internet ne devrait être possible qu'au cas par cas, avec le nom et le prénom. A propos des problèmes et des risques pratiques inhérents aux différentes orthographes des noms, nous avons suggéré d'améliorer les critères de recherche quant à l'orthographe et à la phonologie des noms et des prénoms. Nous avons également suggéré qu'un accès élargi (avec mot de passe) soit créé pour certaines organisations. Les personnes qui ne disposent pas d'accès Internet ou qui ont des difficultés à utiliser Internet pourront s'adresser à ces organisations pour

procéder à leurs recherches. Par ailleurs, la liste entière sur papier peut être remise à ces mêmes organisations afin de permettre la consultation complète de la liste telle qu'elle a été demandée.

L'Association suisse des banquiers a donné mandat à une société fiduciaire de procéder au traitement et à la publication des données. Nous avons attiré l'attention de l'Association suisse des banquiers sur le fait qu'en tant que maître du fichier, elle en conservait la responsabilité et que le traitement et la publication de ladite liste devaient avoir lieu dans le respect de la législation suisse en matière de protection des données.

5. Communication de données personnelles

5.1. Annuaires en ligne des collaborateurs de l'administration fédérale (Admin Directory Public)

A l'âge de l'Internet, l'«annuaire fédéral» bien connu sous forme de livre va également devenir disponible en version électronique. Le but est - dans un souci de rendre l'administration transparente et conviviale pour les citoyens - de faciliter et surtout d'accélérer l'accès aux informations relatives aux autorités fédérales et à leurs collaborateurs. Il importe cependant de respecter les dispositions de la protection des données prévues pour protéger les personnes concernées.

La publication de données personnelles dans l'Intranet de l'administration fédérale ou dans l'Internet est une communication par procédure d'appel effectuée par un organe fédéral qui nécessite - selon la loi sur la protection des données – une base légale. Une telle base pour la publication d'annuaires permettant de faciliter la communication entre les collaborateurs de l'administration fédérale est prévue dans l'ordonnance sur l'organisation de la Chancellerie fédérale. Celle-ci permet en particulier de rendre accessible *au sein de l'administration fédérale* pour la publication électronique d'annuaires les données suivantes de l'ensemble des collaborateurs: nom, prénom, fonction, titre, langue officielle utilisée, numéros de téléphone, de télécopieur et de «pager», adresses postales et électroniques, protocoles de communications utilisés et certaines données de cryptage. De tels annuaires en ligne existent déjà depuis plusieurs années dans l'Intranet de l'administration fédérale.

En ce qui concerne les annuaires électroniques qui sont prévus pour un *accès depuis l'extérieur de l'administration* (par ex. dans le cadre du projet «Admin Directory Public» de l'Office fédéral de l'informatique et de la télécommuni-

cation), l'accès doit être restreint aux données des «collaborateurs qui sont les interlocuteurs directs des tiers». Cette restriction est ancrée dans l'ordonnance sur l'organisation de la Chancellerie fédérale. Elle découle des principes de finalité et de proportionnalité.

Il est très important que les organes fédéraux soient informés sur les risques inhérents à une publication sur Internet (accès possible également depuis des pays où les dispositions en matière de protection des données sont rudimentaires ou inexistantes, mise en relation facile avec d'autres données, manque de sécurité des données). Des critères uniformes doivent être appliqués au niveau fédéral pour apprécier si une personne doit être considérée comme «interlocuteur envers des tiers» ou non.

Suite aux contacts que nous avons eus jusqu'ici avec les organes concernés de la Chancellerie fédérale et de l'Office fédéral de l'informatique et de la télécommunication, nous sommes confiant qu'une solution pourra être trouvée qui réponde de manière optimale autant aux intérêts des interlocuteurs de la Confédération qu'à la protection des données des collaborateurs.

6. Protection des données et conditions légales cadres

6.1. Gouvernement électronique et exigences minimales pour la protection des données

La cyberadministration sera bientôt une réalité pour le citoyen. Sous le nom de gouvernement électronique, des projets d'envergure tels que le guichet virtuel et le vote électronique sont en train de voir le jour. Ce formidable défi technologique pose avec une nouvelle acuité la question de la protection de la sphère privée. Si l'information demeure l'objectif principal du guichet virtuel, les communications et les transactions vont se développer également, notamment dans le cadre du vote électronique. La confiance du citoyen dans la cyberadministration sera un facteur primordial de réussite pour le gouvernement électronique. Ces projets ambitieux doivent être exemplaires quant au respect des principes de la protection et de la sécurité des données. Ils devront également promouvoir des technologies novatrices, toujours plus respectueuses de la sphère privée.

La Chancellerie fédérale conduit deux projets clefs dans le domaine du gouvernement électronique, à savoir la création d'un guichet virtuel et la mise en œu-

vre du vote électronique. Un groupe de travail «Guichet virtuel», institué en juin 2000, a été chargé d'évaluer les divers concepts de guichets virtuels existants en Suisse et à l'étranger. Il a également rédigé un projet de convention de collaboration entre la Confédération et les cantons en vue de l'élaboration d'un guichet virtuel. La convention a été signée en décembre 2000.

Le succès du projet de vote électronique, envisagé dans une étape ultérieure, dépendra pour une bonne part de la qualité et du bon fonctionnement du guichet virtuel. Par conséquent, il est impératif de jeter dès maintenant les meilleures bases en matière de protection des données.

Le guichet virtuel vise la conception et la réalisation d'un système informatique basé sur Internet permettant un accès simple et intuitif aux prestations des administrations fédérales, cantonales et communales. Il ne remplacera pas les sites web actuels. Cette plate-forme offrira des liens vers les informations des cantons et des communes. L'accès se fera par l'intermédiaire de thèmes (auto, impôts, naissance, mariage, divorce, retraite etc.). Après une brève explication, l'utilisateur sera guidé directement vers les pages Internet des services compétents de la Confédération, des cantons ou des communes.

Il est important que les concepteurs du projet arrêtent leur politique de protection des données aussitôt que possible. Il s'agit en particulier de procéder aux choix suivants:

- les mandats en matière de protection des données doivent-ils être attribués au secteur public ou au secteur privé?
- quelles sont les technologies existantes à privilégier?
- quels sont les secteurs où il faut prévoir d'investir?
- où doivent se situer les interfaces du système?
- souhaite-t-on développer un concept de protection des données centralisé ou décentralisé, suisse ou international (nombre et configuration géographique des différents éléments du système de protection tels que firewall, autorités de contrôle et de certification, fonctions des administrateurs)?

Le cadre légal du guichet virtuel doit être minutieusement choisi (loi, ordonnances, directives, conventions et contrats). Pour être adéquat, celui-ci devra tenir compte de la législation actuelle sur la protection des données et du caractère innovateur du projet (sont également concernées les nouvelles notions juridiques de certification et signature électronique par exemple). Par ailleurs, les cantons et les communes, partenaires essentiels du projet, vont inéluctablement se trouver confronter à l'effet centralisateur lié au développement de la technologie sur Internet et la difficulté de l'exercice n'est pas à sous-estimer. Seul un cadre légal clair permettra de définir suffisamment tôt les éventuelles nouvelles répartition de compétence. Ces questions devraient, à notre sens, faire l'objet d'une loi au sens formel.

Les grandes options techniques doivent êtres décrites dans un règlement de traitement. Ce document prévu par l'ordonnance relative à la loi fédérale sur la protection des données fixe la planification, ainsi que les grandes lignes techniques et organisationnelles liées à l'ensemble du processus. Ce règlement doit être élaboré au début du projet et être régulièrement mis à jour par la suite. HERMES, l'instrument de gestion élaboré par l'Office fédéral de l'informatique et de la télécommunication pour les projets électroniques au sein de la Confédération, offre une base utile à l'élaboration d'un tel règlement de traitement.

Au vu de l'ampleur du processus, il conviendrait d'élaborer un module de formation axé sur la problématique de la protection des données et visant à sensibiliser constamment et à tous les stades les acteurs impliqués dans les projets en cause.

Le guichet virtuel comportera un aspect «information» (ou s'adresser pour tel ou tel sujet de la vie courante, à quelles heures etc.), ainsi qu'un aspect «communication» et «transaction» (échanges de formulaires administratifs, paiements, délivrance d'attestations diverses etc.). Dans le premier cas de figure, ce sont les questions liées à la traçabilité des utilisateurs (personnalisation par le numéro IP, coockies, établissement de profils, conservation des données etc.) qui prédominent . Dans le second cas de figure, les problématiques liées aussi bien à la confidentialité, à l'intégrité qu'à l'authentification des opérations, se posent en plus de celle de la traçabilité.

Dans la réalisation du gouvernement électronique, il devra être tenu compte, en particulier, des principes généraux de protection des données suivants:

- la proportionnalité et la finalité: l'accès à l'information ne doit pas entraîner la collecte et le traitement de données personnelles supplémentaires à celles qui sont nécessaires pour répondre aux demandes de l'utilisateur ou à celles que ce dernier est tenu de communiquer de par la loi (déclaration fiscale, demande de subvention etc.);
- la concentration et la centralisation des données: celles-ci ne doivent pas être accrues sous prétexte de rationalisation et d'harmonisation; une attention particulière sera faite au risque de flux de données entre la Confédération, les cantons ou les communes, de même qu'à l'intérieur d'une même administration;
- la transparence: chaque fois que des données personnelles lui sont demandées, l'utilisateur doit pouvoir librement et de manière éclairée se déterminer avant de les communiquer; les éléments suivants doivent lui être communiqué lors de toute opération: la finalité, les destinataires, les éléments facultatifs ou nécessaires (à signaler de manière distincte), les coordonnées des maîtres de fichiers et la durée de conservation des données;

- le droit d'accès: l'utilisateur doit pouvoir, à tout moment, contrôler les données enregistrées à son sujet, demander leur suppression ou leur rectification;
- l'accès anonyme: l'utilisateur qui le souhaite ne doit pas pouvoir être tracé dans ses recherches (notamment par son numéro IP ou des coockies); le recours aux pseudonymes, ainsi qu'aux technologies de la vie privée (PET) doit être encouragé toutes les fois que c'est possible;
- publication des données: toute publication relative à des données personnelles doit être licite;
- pour les communications et les transactions, la confidentialité, l'intégrité et l'authentification de données doivent être garanties; il conviendra de recourir aux dernières technologie de cryptage, certificat et signature électronique.

6.2. Lutte contre le travail au noir

La mise en réseau (accès en ligne à l'ensemble des fichiers existants ou comparaison de ces fichiers) de données administratives (fisc, assurances sociales, police des étrangers et asile) doit être conforme aux principes généraux de protection des données. Une telle mesure va entraîner de nombreuses communications de données sensibles par procédure d'appel devant être prévues expressément par des dispositions légales au sens formel.

Le Conseil fédéral a attribué à un groupe de travail fédéral sur la lutte contre le travail au noir le mandat, entre autres, d'analyser la faisabilité juridique et technique de la mise en réseau des données administratives relatives au fisc, aux assurances sociales (AVS, AI et assurance-chômage), à la police des étrangers et à l'asile. Une telle mesure a pour objectif de rendre les données administratives accessibles aux organes de contrôle chargés de la détection des cas de travail au noir. Par mise en réseau on entend, d'une part, la possibilité d'avoir accès par procédure d'appel à des informations contenues dans différents fichiers et, d'autre part, la comparaison systématique des données qui figurent dans l'ensemble de ces registres. Dans le cadre de ce mandat, nous avons rappelé que tout traitement de données personnelles doit être conforme aux principes généraux de protection des données.

L'examen de la conformité d'un traitement de données personnelles au principe de proportionnalité se déroule en deux étapes. En premier lieu, il faut se demander si les données personnelles que l'on entend traiter sont nécessaires et aptes à atteindre le but recherché à savoir, dans le cas d'espèce, la lutte contre le travail au noir. Le groupe de travail a constaté que les données disponibles posaient de sérieux problèmes de comparabilité du point de vue de leur contenu et de leur actualité. De plus, certaines données contenues dans les banques de données

analysées ne fournissent pas des informations pertinentes pour l'identification de situations de travail au noir. Dans un deuxième temps, il faut procéder à une pesée des intérêts entre le but du traitement, notamment les résultats attendus, et l'atteinte à la personnalité des personnes concernées. Dans une mise en réseau générale, il faut être conscient qu'un volume immense de données personnelles concernant une très grande partie de la population résidant en Suisse serait traité avec pour conséquence une augmentation des risques liés à la sécurité des données. Des données personnelles sensibles et des profils de la personnalité seront traités par plusieurs organes fédéraux et cantonaux. Ces traitements, en particulier les communications par procédure d'appel, devront être expressément prévus par des dispositions légales au sens formel. Les bases juridiques devront définir le but du traitement, décrire dans les grandes lignes l'importance du traitement, désigner les organes qui participent au traitement et désigner les catégories de données traitées. Les législations sur les assurances sociales, sur le fisc et sur les étrangers devront ainsi être modifiées dans ce sens.

Le groupe de travail est parvenu à la conclusion que la mise en réseau générale des registres existants ne permettrait pas véritablement d'augmenter l'efficacité de la lutte contre le travail au noir et que les traitements envisagés paraissaient disproportionnés en regard de l'objectif visé. Il a par conséquent proposé une mise en réseau limitée au domaine des assurances sociales (comparaisons des données de l'assurance-chômage avec celles de l'AVS). En tant qu'organe de conseil, nous suivrons l'évolution de ce projet et nous nous prononcerons dans le cadre des consultations relatives aux adaptations de dispositions déjà existantes ou à la création de nouveaux textes légaux dans ce domaine.

7. Protection et sécurité des données

7.1. Algorithmes de chiffrement considérés aujourd'hui comme sûrs

Les procédés ou algorithmes de chiffrement sûrs doivent être publiés afin d'assurer la transparence. Une telle publication permet également aux experts de tester les procédés qui ont été publiés. Les algorithmes symétriques avec une longueur de clé de 128 bits et les algorithmes asymétriques avec des longueurs de clé de 1024 ou 2048 bits sont aujourd'hui considérés par le Préposé fédéral à la protection des données comme étant sûr.

Le Préposé fédéral à la protection des données reçoit régulièrement des demandes pour savoir quels sont les procédés de chiffrement qu'il considère comme étant sûr. Il y a lieu de relever qu'en principe la publication d'un algorithme de

chiffrement constitue toujours un avantage car elle permet à d'autres experts du chiffrement de tester ces algorithmes et de signaler les éventuels points faibles. En outre, elle garantit un maximum de transparence. Nous ne doutons pas qu'il existe également de bons algorithmes parmi ceux qui n'ont pas été publiés. On est cependant en droit de se poser les questions pourquoi ces algorithmes n'ont pas été publiés et pour quelle raison on ne désire pas créer la transparence. Les algorithmes non publiés présentent le risque qu'ils contiennent des «échappatoires» qui permettent par exemple à d'autres organismes ou autorités de déchiffrer les données ainsi chiffrées. Parmi les procédés de chiffrement symétriques on considère aujourd'hui comme sûrs les algorithmes publiés avec une longueur de clé de 90 bits au moins, tel que par exemple l'algorithme IDEA (International Data Encryption Algorithm) avec une longueur de 128 bits ou l'algorithme Triple DES (Data Encryption Standard). En ce qui concerne les algorithmes asymétriques tels que l'algorithme RSA (Rivest, Shamir, Adleman), la clé à 512 bits a pu être «cassée» en 1999. On part aujourd'hui du principe qu'une longueur de clé de 1024 bits peut être considérée comme sûre. De notre côté, nous faisons preuve de précaution et conseillons donc aux utilisateurs d'utiliser des clés aussi longues que possibles.

7.2. Mots de passe sûrs et autres procédés d'authentification

Un mot de passe devrait avoir une longueur de 6 caractères au moins (8 ou plus sont conseillés). Il existe des outils simples permettant de générer de tels mots de passe et de les mémoriser de manière à ce que le mot de passe puisse être régénéré même après une longue absence. Il faut veiller à ce qu'un mot de passe soit modifié de manière périodique (par ex. tous les 3 mois). Les experts sont d'avis que pour les environnements sensibles notamment une authentification basée sur la connaissance (mot de passe) n'est pas assez sûre et que d'autres procédés complémentaires telles que des cartes à puce ou des systèmes biométriques devraient être mis en œuvre.

Pour s'identifier auprès d'un système informatique, on utilise de nos jours la plupart du temps une identification d'utilisateur (USER ID) ainsi qu'un mot de passe. Il faut veiller lors du choix du mot de passe à ce que celui-ci ait une longueur de 6-8 caractères au moins. On utilise d'ailleurs, surtout dans le monde anglophone, également le terme de «passphrase» (phrase de passe). Ce terme devrait nous rappeler que, pour des raisons de sécurité, nous ne devrions pas utiliser un simple «mot», mais plutôt une combinaison de caractères dénuée de sens qui donne facilement une longueur de 8-12 caractères.
Un aspect très important lors du choix du mot de passe est d'éviter d'utiliser des mots tels que nom, prénom, numéro de plaque d'immatriculation, numéro de

téléphone ou autres combinaisons de caractères telles que celles mentionnées dans le dictionnaire. Si l'on intercale ensuite des chiffres et des caractères spéciaux tels que % ou & entre les lettres, on obtient ce qu'on appelle un «bon» mot de passe. Un tel mot de passe aura peu de chance d'être découvert en utilisant les outils «pirates» qui peuvent être gratuitement téléchargés depuis l'Internet.

Un des plus gros soucis des utilisateurs est qu'ils risquent d'oublier leur mot de passe. Le fait de ne pas utiliser certaines connaissances pendant une période prolongée présente le risque qu'on les oublie. Il se peut donc que l'on ne se souvienne plus du mot de passe en rentrant des vacances. C'est la raison pour laquelle on est tenté de noter le mot de passe quelque part. On aimerait à tout prix éviter d'être la personne qui doit constamment appeler l'administrateur système pour lui demander de créer un nouveau mot de passe. Il est un principe qu'un mot de passe ne doit jamais être accessible publiquement ni conservé en clair. On peut envisager les solutions suivantes: nous notons sur un bout de papier une ou plusieurs phrases qui n'ont aucun rapport avec l'informatique. Nous choisissons alors une des phrases pour créer notre mot de passe. Nous mémorisons (sans le noter sur le bout de papier) le système de clé qui consiste à utiliser les deux dernières lettres de chaque mot de la phrase pour former le mot de passe. Nous complétons ensuite ce mot de passe par des caractères spéciaux et utilisons deux des lettres dans leur forme majuscule.

Exemple:
(phrase notée) ⇒ **Il** faisa**it** be**au** hi**er** ⇒ mot de passe **= ilitauer**
Nous y ajoutons des caractères spéciaux pour obtenir **£ilitauer$**
puis mettons les deux lettres du milieu en majuscule, ce qui donne finalement **£iliTAuer$**.

Une autre méthode consiste à créer une carte contenant des caractères quelconques que l'on utilise ensuite pour créer un mot de passe à l'aide d'une clé ou de critères de sélection.

Exemple:

	1	2	3	4	5	6	7	8	9	0
1	a	b	h	i	Z	£	?	P	k	ö
2	C	&	%	I	7	h	F	f	ä	j
3	)	Q	B	%	n	L	&	8	L	D
4	1	4	D	g	g	L	9	3	N	m
5	&	#	#	K	K	l	o	g	$	!

6	Z	+	I	9	0	&	L	b	*	7
7	W	6	!	F	h	B	7	3	v	V
8	G	G	K	?	m	k	$	@	A	m
9	z	8	h	M	)	ç	x	K	9	0
0	(	¢	v	7	2	l	K	ä	m	q

On peut par exemple se souvenir du chiffre 45 puis utiliser le tableau pour créer le mot de passe en prenant tous les caractères depuis le chiffre 4 en haut jusqu'à l'intersection avec le chiffre 5 (5ème rangée), puis en continuant vers la droite (ou la gauche ou en diagonale) jusqu'à ce que l'on ait obtenu 8 caractères. Dans le tableau ci-dessus, ceci donnerait: **iI%gKK1o .**
Cette carte (ou les phrases citées plus haut) peuvent par exemple être conservées dans le portefeuille. Au cas où le portefeuille devait être volé, les mots de passe doivent être immédiatement modifiés et de nouvelles phrases ou cartes doivent être créées.

Cette méthode permet de gérer un nombre limité de mots de passe. Si vous utilisez plusieurs mots de passe, il est indiqué d'utiliser un outil permettant de gérer les diverses identifications d'utilisateur et mots de passe (tel qu'un «Single Sign On Systeme»).

Un mot de passe doit être modifié périodiquement (environ tous les 3 mois) et il faut absolument éviter de réutiliser l'ancien mot de passe.

Certains experts rendent attentifs au fait qu'un mot de passe seul, qui permet une authentification basée sur la connaissance, n'est pas assez sûr dans des environnements sensibles. C'est pourquoi ils proposent de prévoir dans de tels environnements l'utilisation (accessoire) de systèmes biométriques (authentification basée sur des caractéristiques propres à la personne) ou de cartes à puce (authentification basée sur la possession). Le thème suivant contient également des informations sur la biométrie.

7.3. Accès aux systèmes informatiques par authentification biométrique

L'étude menée par une école d'ingénieurs mandatée par le PFPD tend à démontrer que les systèmes d'authentification par empreintes digitales sont aujourd'hui techniquement au point et remplacent avantageusement l'authentification classique par mots de passe. Quelques lacunes de sécurité au niveau de leur intégration dans les systèmes d'exploitation ont néanmoins été constatées. Ces défauts de jeunesse disparaîtront bien vite, car

ces nouvelles techniques d'authentification biométrique constituent le seul espoir de progrès dans le domaine de la sécurité d'accès aux innombrables services électroniques proposés sur le marché.

Avec l'informatisation croissante de notre société, chaque personne est amenée à mémoriser un nombre impressionnant de mots de passe, codes d'identification personnelle (PIN: Personal Identification Number) et autres sésames. Certains de ces codes doivent de surcroît être modifiés à intervalles réguliers, afin de limiter les risques d'utilisation abusive par des personnes entrées illicitement en possession de ces éléments de sécurité. En réponse à cette sollicitation, l'utilisateur a la fâcheuse habitude de simplifier et/ou uniformiser ses codes d'accès, voire même de les inscrire sur un morceau de papier souvent entreposé à proximité du service proposé (mots de passe sous le clavier, PIN sur la carte de crédit...). Cette réaction affaiblit malheureusement d'une manière considérable la sécurité d'accès aux services concernés et il y a lieu de trouver des solutions convaincantes à ces problèmes. L'utilisation de logiciels, disponibles parfois même gratuitement, permettant de gérer un ensemble de codes personnels dans une base de données cryptée, représente déjà un très net progrès par rapport à une liste sur papier. De manière analogue, on peut utiliser la zone confidentielle d'un assistant digital personnel (PDA: Personal Digital Assistant) que l'on porte en principe toujours sur soi.

Il n'en reste pas moins que ces codes sont pour la plupart simples et en relation directe avec l'utilisateur, son entourage ou ses habitudes, de sorte qu'ils peuvent être facilement découverts par des tiers mal intentionnés. C'est dans ce domaine que l'authentification biométrique apporte une contribution majeure, puisqu'elle exploite un trait physique propre à l'utilisateur plutôt qu'un code mémorisé et reproduit par celui-ci. Les traits physiques personnels utilisables sont évidemment très variés, ce qui implique une complexité et une fiabilité de reconnaissance également très variables. Les caractéristiques physiques les plus utilisées pour l'authentification biométrique sont les suivantes: empreinte digitale, timbre vocal, morphologie de la main, du visage ou de l'oreille, motif de l'iris ou de la rétine, apparence et/ou dynamique de la signature manuscrite, dynamique de la frappe au clavier, composition sanguine, odeur corporelle.

La préférence des utilisateurs va évidemment aux méthodes qui ne dépendent pas de leur état physique ou émotionnel, ne nécessitent aucun contact physique et ne présentent pas de risque en matière de protection des données. Certaines méthodes induisent en outre un reflex naturel de crainte: l'empreinte digitale qui a une connotation policière, les motifs de la rétine ou de l'iris qui sont indirectement porteurs d'informations sur l'état de santé de la personne authentifiée. La question sous-jacente est bien évidemment celle du respect de la finalité de l'exploitation de ces caractéristiques personnelles.

A ce stade, il est très important de mentionner que les systèmes d'authentification biométrique transforment en principe la caractéristique physique analysée en un gabarit (template) nettement mieux adapté à la comparaison. Il faut ainsi garder à l'esprit qu'aucune méthode d'authentification biométrique n'est absolue, puisque la reconnaissance a lieu par une évaluation probabiliste de la correspondance entre le gabarit analysé et une base de données de gabarits de référence. Chaque méthode est ainsi caractérisée par le taux de fausses acceptations (confidentialité et intégrité en péril) et le taux de faux rejets (disponibilité et fiabilité en péril) qui dépendent tous deux de la «différentiabilité», reproductibilité et durabilité des traits physiques choisis, sans oublier les facteurs externes que sont le prix des équipements et le niveau d'acceptation par les utilisateurs.

A l'exception du dernier critère, l'authentification par empreintes digitales est sans conteste celle qui fournit le meilleur rapport qualité/prix, comme en témoigne l'explosion de l'offre de produits ayant recours à cette technologie. L'image d'une empreinte digitale est transformée en un gabarit formé de coordonnées de minuties qui sont des points spécifiques et propres à chaque empreinte (terminaisons, jonctions, arcs, boucles, volutes...). Afin d'augmenter la fiabilité du système, le gabarit conservé est le résultat moyen d'une série d'empreintes du même doigt et il est souvent même complété par des gabarits issus d'autres doigts de l'utilisateur. En ce qui concerne les possibilités de falsification, certains lecteurs d'empreinte sont sensibles à la chaleur et au contact, ce qui évite les tromperies par apposition d'images. Il est néanmoins clair qu'un tel système pourrait théoriquement être abusé par une sorte de peau artificielle gravée selon une empreinte acquise à l'insu d'une personne ciblée, mais il faut toujours comparer les coûts d'une telle opération avec le bénéfice que l'on peut en tirer.

Comme la transformation d'une empreinte digitale en un gabarit est irréversible, il n'y a aucun risque de reconstitution d'empreinte à partir d'un gabarit, et du fait que cette transformation n'est à l'heure actuelle pas du tout standardisée, il n'y a que très peu de risques de mise en relation, par le biais de gabarits correspondants, de bases de données censées rester indépendantes. Pour garantir cette indépendance qui préserve en fait la pseudonymité de l'utilisateur, il faut soit recourir à des caractéristiques physiques différentes pour chaque service, soit crypter individuellement chaque base de gabarits ou empreintes.

L'étude réalisée s'est concentrée sur ce type d'authentification, en particulier sur des lecteurs d'empreintes digitales intégrés à la souris, au clavier ou à un périphérique dédié d'un ordinateur. Si la partie d'acquisition et de reconnaissance des empreintes n'a jamais vraiment posé de problèmes, l'intégration du logiciel dans les couches de sécurité du système d'exploitation a par contre conduit à bon nombre de désillusions. La base de gabarits doit inévitablement être mise en relation avec celle des mots de passe des personnes identifiées (base SAM de

Windows NT par exemple). Dans un cas, cette correspondance a carrément été réalisée par une copie des mots de passe figurant ensuite en texte clair et éditable! dans la base de gabarits. Cette lacune rédhibitoire fait regretter les avantages offerts par l'identification automatique (plus besoin d'introduire son nom d'utilisateur) et par la possibilité d'utiliser les empreintes digitales comme clés de cryptage pour des fichiers personnels sensibles. Dans un autre cas, les bases de données étaient bien séparées, mais leur liaison permettait de remplacer les gabarits d'une personne par les siens et gagner par là même l'accès au système sous l'identité et avec tous les privilèges de la personne ainsi piégée. Seul le lecteur d'empreinte faisant partie d'un périphérique dédié a permis une authentification sûre et fiable, associée à une identification automatique des utilisateurs. Une attaque du canal de communication (en l'occurrence USB) entre le périphérique et l'ordinateur resterait vaine, étant donné qu'un codage dynamique des empreintes transmises est effectué. Pour ce lecteur dédié, il existe en outre une extension logicielle pour serveurs NT qui permet de substituer entièrement les mots de passe par des gabarits dérivés d'empreintes digitales personnelles. La gestion centralisée de ces gabarits permet la mobilité (roaming) des utilisateurs, puisqu'ils peuvent alors être authentifiés et identifiés sur n'importe quel poste muni d'un lecteur approprié. Dans le cas des souris dotées de lecteurs d'empreintes digitales, il faut par ailleurs reconnaître que les deux modèles testés n'offraient pas vraiment les qualités fonctionnelles et ergonomiques (pas de roulette, cordon trop court, mauvais contact des touches...) que l'on attend aujourd'hui de tels dispositifs de pointage. Les claviers devraient moins prêter le flan à de telles critiques, étant donné que leur ergonomie est quasiment standardisée et que la qualité de leur fonction première, à savoir le confort de frappe, n'est que rarement remise en cause.

En conclusion, l'étude a démontré que l'authentification par empreintes digitales est aujourd'hui parfaitement réalisable. Par rapport à l'authentification par mots de passe, on constate un gain indiscutable tant du point de vue du confort d'utilisation que du point de vue de la sécurité, pour autant que cette dernière soit assurée d'une manière globale. Une diffusion à large échelle de ces dispositifs d'authentification biométrique contribuera certainement à abaisser leur prix et surtout à améliorer le niveau général de sécurité et de protection des données.

7.4. Journalisation de données relationnelles: finalité, protection, archivage et destruction

Depuis quelques décennies, on constate une prédominance du modèle relationnel dans l'univers des bases de données. La journalisation du traitement de telles données représente, même lorsqu'elle est dûment motivée, une difficulté technique et organisationnelle non négligeable. Fort heureusement, les outils standards mis à disposition par les systè-

mes relationnels permettent d'apporter des solutions satisfaisantes à ces problèmes. Vu la sensibilité des données de journalisation, il est absolument nécessaire d'assurer leur confidentialité et leur intégrité, dans le cadre d'une politique cohérente d'archivage et de destruction.

Dans le contexte des systèmes de bases de données relationnelles (plus loin SGBDR), le langage ISO/SQL (International Standards Organisation, Structured Query Language) comprend la très ancienne et célèbre instruction d'interrogation «SELECT FROM WHERE», ainsi que les trois instructions de mise à jour «INSERT, UPDATE, DELETE» pour respectivement ajouter, modifier et détruire des données dans une table d'un schéma relationnel. Dans ce contexte, la journalisation consiste simplement à insérer pour chaque opération effectuée un enregistrement contenant les informations «Who did What, When» dans une table additionnelle, idéalement localisée dans une base de données indépendante et réservée à cet usage. Afin de permettre une analyse anonyme des tables de journalisation, il est recommandé de mémoriser les informations d'identification personnelle («Who») sous une forme cryptée.

Pour la journalisation des interrogations de données, c'est en fait l'application qui doit prévoir explicitement de parapher chaque lecture par une insertion dans le journal correspondant. Cette contrainte a au moins le mérite de soulever la question de la finalité d'une telle démarche, en gardant surtout à l'esprit que certaines tables peuvent faire l'objet d'un nombre impressionnant de lectures journalières.

Pour la journalisation des mises à jour par contre, le standard SQL permet de définir des «TRIGGERS» qui sont en fait des petits programmes de mises à jour annexes, déclenchés avant ou après l'accomplissement d'une mise à jour principale. Il suffit ainsi de définir, sur chaque table concernée, un TRIGGER pour chacune des trois instructions de mise à jour [exemple: CREATE TRIGGER tr_client_up FOR client AFTER UPDATE AS INSERT INTO log_client SELECT Who, When, ClientNum, PhoneNum... FROM Inserted;], pour que le SGBDR assure une journalisation automatique et totalement indépendante de l'application.

S'agissant des privilèges d'accès aux tables de journalisation (SQL: GRANT), il est évident que l'ajout d'enregistrement doit être accordé à tous les utilisateurs (SQL: Public) et que toute possibilité de modification ultérieure doit être strictement prohibée. Les responsables de la sécurité des données doivent par contre pouvoir consulter ces journaux et à l'occasion les vider après leur transfert périodique sur supports d'archivage. Ces supports d'archivage doivent eux aussi être finalement détruits, après que le délai maximal de conservation prescrit est atteint.

Comme pour toute destruction de données sensibles, il y a lieu de procéder à une élimination physique, par opposition à l'effacement logique assuré par les outils communément mis à disposition. Pour les fichiers traditionnels, on peut recourir à des utilitaires de destruction (file wiping tools) opérant par réécritures multiples. Avec les bases de données relationnelles, la destruction physique du contenu d'une table est nettement moins évidente, du fait de la gestion automatique de l'espace de mémorisation. Une réorganisation complète, une compression ou un rechargement de la base de données peut être nécessaire, à moins que l'instruction DELETE n'offre une option propriétaire garantissant la destruction physique des données.

On voit donc que les systèmes de gestion de bases de données relationnelles offrent toutes les fonctionnalités pour effectuer de manière simple, autonome et en partie même indépendante de l'application, une journalisation des traitements effectués. Ces systèmes permettent également de définir une sécurité d'accès à ces informations répondant pleinement aux exigences en matière de protection des données. Accompagnée par une politique sérieuse d'archivage, puis surtout de destruction des données, la journalisation de données relationnelles finit par être moins compliquée et dangereuse qu'il n'y paraît au premier abord.

7.5. EDSB-Office: notre système sécurisé de gestion des affaires

Après plus d'une année d'expérience avec une infrastructure interne à clés publiques, le PFPD livre quelques conclusions quant à la faisabilité, à l'introduction et à l'évolution d'un tel système. Les résultats atteints en matière de sécurité, de performance et de praticabilité démontrent que la technologie actuelle permet de réaliser des environnements hautement sécurisés, en toute conformité avec les exigences les plus élevées de notre loi sur la protection des données.

Suite à l'incompatibilité de notre ancien système avec l'an 2000 et dans le but avoué de démontrer la faisabilité d'un système permettant de crypter tous les documents de travail, le PFPD a fait développer une application Windows spécifique, mais néanmoins basée sur «la suite bureautique» et un système de gestion de bases de données relationnelles couramment utilisés dans le marché. Dans un cadre clients-serveur aujourd'hui traditionnel, les opérations de cryptage et décryptage sont effectuées sur chaque client à l'aide d'un logiciel ad hoc, qui s'est par ailleurs imposé comme standard de fait pour le traitement des messages électroniques cryptés. Les documents et champs sensibles sont ainsi transmis de manière inviolable entre les clients et le serveur de bases de données, où ils sont mémorisés sous cette forme cryptée, afin d'assurer leur sécurité

par rapport à toutes les attaques à ce niveau-là (intrusions, bandes de sauvegarde...). Les documents envoyés sur une imprimante branchée sur le réseau bénéficient d'une protection similaire, grâce à des serveurs d'impression assurant le décryptage des flux imprimables immédiatement avant le tirage sur papier proprement dit. Pour les documents très sensibles, une imprimante branchée localement sur le poste du rédacteur est naturellement préférable.

L'expérience démontre que les temps de réponse pour les opérations de cryptage et décryptage sont entièrement satisfaisants pour des documents contenant jusqu'à plusieurs dizaines de pages. Un gain de place est réalisé au passage, étant donné que le cryptage implique une compression automatique des documents. Dans un contexte d'infrastructure à clés publiques (PKI: Public Key Infrastructure), la gestion des clés a constitué un élément crucial du projet. La génération des clés asymétriques (paires formées d'une partie publique et d'une partie privée) est réalisée directement par les utilisateurs, de façon à éviter toute possibilité de copies illicites des éléments sensibles. Leur conservation est assez paradoxalement prévue sur une simple disquette, dont l'accès est certes un peu lent, mais dont l'amovibilité est un gage certain de sécurité pour un coût quasiment nul (lecteur présent d'office et support extrêmement avantageux). D'autres types de support amovible plus rapides, plus fiables et/ou plus compacts, mais aussi plus onéreux, pourraient bien sûr être utilisés pour la mémorisation de ces trousseaux de clés (keyrings).

Protégeant la partie privée de la clé, l'expression de passe (passphrase) revêt une grande importance et sa complexité doit impérativement atteindre un certain niveau (longueur, inintelligibilité, caractères spéciaux...), de façon à résister aux attaques potentielles d'un intéressé. La partie publique de la clé peut et doit, comme son nom l'indique, être librement exportée ou transmise à toute personne qui désire produire un document lisible exclusivement par le détenteur de la partie privée correspondante. Dans un cercle où les personnes se connaissent et se rencontrent souvent, l'échange de clés publiques peut avoir lieu simplement par disquette et ne nécessite ainsi aucune autorité tierce de certification (CA: Certification Authority).

Après avoir introduit l'expression de passe associée à sa clé privée, un utilisateur peut entrer dans l'application pour gérer l'ensemble de ses documents personnels et lire tous les documents cryptés avec la clé de groupe (mode par défaut). Au-delà de cette idée habituelle de clés individuelles et de groupe, le programme prévoit en outre un cryptage de chaque document avec une clé supplémentaire de sécurité jouant le rôle d'une clé additionnelle de décryptage (ADK: Additional Decryption Key). Il s'agit de rester capable en toute circonstance de lire les documents mémorisés, même en cas d'indisponibilité des éléments habituels de décryptage par suite de perte, oubli, détérioration... Cette fonction est dévolue au groupe des membres de la direction et échappe ainsi au contrôle des

administrateurs du système. Cette dissociation des rôles reste malheureusement l'exception dans le monde de la gestion des données.

Dans ce contexte de documents cryptés, il faut encore relever la propriété remarquable offerte par la recherche d'un document au moyen d'une combinaison logique de mots significatifs présents dans son contenu, communément appelée recherche en plein texte. Il va de soi qu'une liste de mots «creux» a été définie dans les quatre langues utilisées (allemand, français, italien et anglais), de façon à alléger les opérations d'indexation et surtout à accélérer le processus de recherche. Le résultat est saisissant, puisque quelques secondes suffisent pour établir la liste des documents répondant aux critères choisis.

L'application permet en outre de travailler indépendamment avec des données productives ou des données fictives, ce qui évite les risques d'accès inopportun aux données productives lors des démonstrations à des tiers ou des tests de nouvelles versions du logiciel. La base de données fictives offre l'avantage supplémentaire de permettre aux nouveaux collaborateurs de prendre contact avec l'application dans un environnement sans risque. S'agissant des nouvelles versions du logiciel, nous avons fait une distinction entre la correction des anomalies qui peut et doit être accomplie le plus rapidement possible et l'amélioration des fonctionnalités qui doit être planifiée, évaluée puis réalisée à une rythme semestriel ou annuel. Ce mode de faire permet une progression efficace, tout en préservant l'indispensable stabilité dont une telle application a besoin.

Le logiciel de cryptage choisi permet en outre à chaque utilisateur d'échanger des messages électroniques chiffrés, ainsi que de se protéger contre les cyberattaques au moyen d'un pare-feu (firewall) personnel ou d'un système de détection d'intrusions. Combinée à un logiciel anti-virus dont les fichiers de définition sont régulièrement mis à jour, cette solution offre un niveau de sécurité adapté aux risques désormais encourus par des stations reliées à l'Internet.

Enfin, ce programme de gestion des affaires offre des fonctions complémentaires de base pour le cheminement des documents (workflow), la planification du travail et la gestion de projets, de même que pour la journalisation exhaustive des opérations de lecture ou écriture de données.

7.6. Application de la sécurité des données dans l’administration fédérale

La sécurité des données doit déjà être prise en charge dans les étapes de planification d’un projet (étude préliminaire, concept). La planification et la réalisation de projets au sein de l’administration fédérale doit se faire conformément au manuel HERMES. Malheureusement, les directives de ce dernier ne sont pas toujours suivies. Le résultat est

qu'un grand nombre des avantages que procurerait une telle norme ne sont pas exploités. Si l'on découpe la sécurité des données en 3 domaines, la confidentialité, la disponibilité et l'intégrité, on constate que les résultats au niveau de la disponibilité au sein de l'administration fédérale sont assez satisfaisants. Par contre, au niveau de la confidentialité et de l'intégrité, certaines mesures doivent encore être prises pour que l'on puisse parler d'une sécurité des données adéquate.

La mise en œuvre de la sécurité des données commence déjà au stade de la planification du système d'information ou système informatique. Tous les projets informatiques de l'administration fédérale devraient être conduits et réalisés en accord avec le manuel HERMES. Ce manuel doit être pris comme standard pour la gestion de projets. Les objectifs de standards peuvent être décrits ainsi:

- indépendant de la personne	-compréhensible	- uniforme
- éviter une prolifération incontrôlée	-qualité avérée	- coûts réduits
- complet	-compatible	- révisable

Nous avons pu constater dans plusieurs cas que l'administration fédérale n'aligne pas sa démarche sur HERMES avec le résultat qu'une grande partie des objectifs cités ci-dessus ne sont pas atteints. Dans une large partie des cas, les consignes de sécurité requises par HERMES et devant être documentées (qualité) ne sont pas suivies. C'est pourquoi nous devons souvent intervenir de manière répétée, dans la mesure ou nous disposons des capacités nécessaires. Les appels d'offres ou cahiers des charges ne contiennent que très rarement des exigences concernant la sécurité des données. Nous avons également pu observer des cas où les appels d'offres ont été effectués sur la base de concepts abstraits qui n'étaient pas basés sur HERMES et qui étaient plutôt flous. Nous ne comprenons pas comment il est possible de porter un choix judicieux sur la base de telles exigences.

Un rapport du Conseil fédéral relève qu'il est difficile de chiffrer le coût de la sécurité informatique. Il précise que cela est principalement dû au fait qu'il est difficile de comptabiliser les frais relatifs à la sécurité séparément des autres frais informatiques. Nous partageons l'avis que les frais encourus pour la sécurité informatique peuvent apparaître à tous les niveaux d'un système ou d'un projet informatique. Nous pensons néanmoins qu'il devrait être possible de constater dans quels domaines de la sécurité les principaux investissements ont été faits. La simple constatation que 6% environ des dépenses informatiques sont liées à des mesures de sécurité des données n'est pas vraiment d'une grande utilité. Il n'est absolument pas clair quels offices ou départements ont investi dans quels domaines de la sécurité des données. Lors de nos interventions à ce sujet en 1999, on a toujours avancé le problème de l'an 2000. Nous

présumons donc que ces moyens ont été utilisés principalement pour l'analyse des systèmes et applications existantes ainsi que pour assurer une exploitation ininterrompue pendant le passage à l'an 2000. Signalons également que le nombre de projets informatiques qui nous ont été soumis ces derniers temps est très bas. Aucun projet traitant principalement d'aspects de la sécurité des données ne nous a été soumis.

Un des domaines de la sécurité des données s'occupe d'assurer l'exploitation du système et de garantir la disponibilité des systèmes et des applications informatiques. Les dépenses pour les mesures nécessaires à cet effet telles que l'achat de systèmes cluster, RAID 5 ou de «shadowing» pour les serveurs ou systèmes hôtes ne devraient plus être imputées aux dépenses pour la sécurité informatique puisque de tels systèmes font aujourd'hui déjà pratiquement partie de l'équipement de base standard. Si un système n'est plus disponible, les services qui en sont concernés s'en rendent compte très rapidement. C'est la raison pour laquelle les mesures de sécurité des données dans ce domaine ont relativement bien été appliquées. Il reste par contre encore beaucoup à faire au niveau de l'intégrité et de la confidentialité des données. C'est dans ce domaine surtout que des éléments de contrôle transparents tels que l'annonce de projets informatiques selon de l'ordonnance relative à la loi fédérale sur la protection des données ou des moyens financiers doivent être mis en œuvre ou imposés afin d'augmenter la sécurité informatique.

Divers contrôles effectués ces derniers mois ont montré qu'il y avait encore beaucoup à faire dans le domaine de la sécurité des données. Si l'on ne met pas à disposition les ressources nécessaires (personnel et moyens financiers), nous craignons que la situation ne s'améliorera pas à l'avenir. Une autre possibilité de résoudre le problème serait, à notre avis, d'octroyer des compétences de sanction plus poussées aux organes de contrôle.

III. ACTIVITÉS INTERNATIONALES

1. Conseil de l'Europe

- Travaux du CJPD: protection des données dans le domaine des assurances et de la vidéosurveillance

Le Groupe de projet sur la protection des données (CJPD) s'est réuni du 9 au 13 octobre 2000. Il a achevé ses travaux dans le domaine des assurances et a poursuivi les travaux entrepris dans le domaine des technologies de l'information, notamment en mettant l'accent sur la surveillance.

Après avoir adopté un projet de recommandation sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (voir 7ème rapport d'activités 1999/200, page 218), le CJPD a finalisé l'exposé des motifs accompagnant ce projet. Le paquet devrait être adopté en 2001 par le Comité des Ministres du Conseil de l'Europe. Le CJPD a examiné un rapport d'expert sur la protection de la vie privée en relation avec la surveillance (http://www.coe.fr/dataprotection) et décidé d'élaborer une série de principes directeurs pour la protection des personnes par rapport à la collecte et au traitement de données au moyen de la vidéosurveillance (voir aussi thème vidéosurveillance, page 189). Partant du constat que de plus en plus d'organismes publics et privés recourent à des systèmes de surveillance, notamment pour contrôler la circulation des personnes et des biens, l'accès aux propriétés ou certaines manifestations, le CJPD estime nécessaire de fixer quelques principes directeurs. Ceux-ci doivent permettre d'étendre et de préciser les garanties qui s'appliquent aux personnes concernées lors de l'utilisation d'installations techniques de vidéosurveillance pour l'observation, la collecte et l'enregistrement de données personnelles concernant en particulier les comportements, les mouvements, les communications d'une ou de plusieurs personnes. Ainsi, selon les propositions de l'expert mandaté par le CJPD, toute activité de surveillance nécessite:

- de vérifier si et dans quelle mesure elle est autorisée sur des bases juridiques appropriées à des fins légitimes, spécifiques et explicites, et si elle est menée de manière loyale;
- de prendre les mesures nécessaires pour veiller à ce que cette activité soit conforme aux principes en matière de protection des données à caractère personnel;
- de n'utiliser des appareils de vidéosurveillance que si l'on ne peut appliquer d'autres systèmes portant moins atteinte à la vie privée;

- de respecter les principes de sélectivité et de proportionnalité concernant les objectifs recherchés dans les cas individuels afin de protéger raisonnablement la vie privée, même dans des lieux publics;
- de respecter le principe selon lequel les données doivent être pertinentes et non excessives, notamment au regard des moyens techniques utilisés;
- de limiter les activités de vidéosurveillance si elles pouvaient conduire à des formes de discrimination ou si elles ont été ordonnées pour certaines personnes exclusivement au regard de leurs opinions, de leurs convictions ou de leur vie sexuelle;
- de respecter le principe de transparence, c'est-à-dire d'informer de l'existence d'une activité spécifique de vidéosurveillance notamment les personnes concernées (en fournissant des informations claires, même sommaires, accompagnées de panneaux signalant de façon visible la localisation des appareils de surveillance);
- de veiller à renforcer la protection en cas de dangers spécifiques pour les personnes concernées et/ou de contrôles plus envahissants (par exemple l'association d'images et de données biométriques ou la définition de profils pour les personnes concernées);
- de ne pas communiquer, en principe, de données à caractère personnel à des tiers qui ne sont pas concernés par l'activité de surveillance;
- de définir des dispositions ad hoc pour l'exercice du droit d'accès et des autres droits des personnes concernées;
- de limiter l'utilisation des systèmes visant à la surveillance délibérée de la qualité du travail et de la productivité sur le lieu de travail et de veiller à ce que les employés soient convenablement informés.

Le CJPD a également examiné le projet de convention sur la criminalité dans le cyberespace et adopté un avis dans lequel il souligne l'importance de la protection des données et demande qu'au minimum une référence à la Convention pour la protection des données à l'égard du traitement automatisé des données à caractère personnel (Convention 108) soit inclue dans le projet de convention. Il rappelle à cet égard que la Convention 108 est partie intégrante des normes constituant l'acquis du Conseil de l'Europe et qu'elle est ouverte à l'adhésion d'Etats non membres du Conseil de l'Europe. Enfin, le CJPD a commencé l'examen d'un projet de recommandation sur l'accès aux documents officiels.

- Travaux du T-PD: protocole additionnel, clauses contractuelles et évaluation de la Convention 108

Le Comité consultatif de la Convention 108 (T-PD) a tenu sa 16ème réunion du 6 au 8 juin 2000. Il a pris note de l'Avis n° 217 (2000) du 5 avril 2000 de l'Assemblée parlementaire relatif au protocole additionnel à la Convention 108 concernant les

autorités de contrôle et les flux transfrontières de données (http://www.coe.fr/dataprotection) et finalisé le texte du protocole additionnel et de l'exposé des motifs. Il a poursuivi ses travaux relatifs aux clauses contractuelles et entamé l'évaluation de la Convention 108 notamment à la lumière des développements technologiques.

Le Comité consultatif a en particulier examiné s'il convenait de modifier le projet de protocole (voir aussi 7ème rapport d'activités 1999/2000, page 219) pour tenir compte des propositions de l'Assemblée parlementaire. Tout en relevant l'apport positif de l'avis de l'Assemblée et notamment son rappel de l'importance de la protection des données à l'heure de l'Internet et de la société de l'information, le Comité n'a pas repris expressément dans le projet de protocole ses propositions. Il s'en est tenu à la ligne qu'il avait définie au début de ses travaux, à savoir rester dans l'esprit et la lettre de la Convention 108 et rédiger un texte limité aux éléments essentiels. En ce sens, certaines des propositions de l'Assemblée ont été intégrées dans le rapport explicatif. D'autres seront examinées ultérieurement.

Le protocole additionnel devrait être prochainement adopté par le Comité des Ministres et ouvert à la signature des Etats membres. La Suisse, qui a activement contribué à son élaboration, devrait être en mesure de le ratifier rapidement. Il faudra examiner la nécessité de modifier la LPD (voir thème vers une modernisation de la protection des données, page 182) pour préciser les compétences des autorités de contrôle et le régime des flux transfrontières de données vers des destinataires non soumis à un régime de protection des données adéquat. Une ratification rapide est dans l'intérêt de la Suisse, notamment en raison des échanges d'information avec l'Union européenne. Dès le moment où les Quinze l'auront ratifié, l'Union européenne pourrait être amenée à revoir son appréciation à l'égard des Etats parties à la Convention 108 qui ne souscriraient pas à ce protocole.

Le Comité consultatif a en outre décidé de procéder à une évaluation de la Convention 108, notamment eu égard aux développements intervenus depuis son adoption il y a 20 ans et aux nouvelles technologies de l'information. Sur la base de cette évaluation, le Comité consultatif déterminera s'il est nécessaire d'envisager un amendement de la Convention 108. Une éventuelle modification ne devrait en aucun cas remettre en cause les principes fondamentaux de la protection des données. Par contre dans l'optique d'un renforcement de la protection des données au niveau international, les compétences de ce comité pourraient être revues.

Le Comité consultatif a également poursuivi l'examen des clauses contractuelles relatives aux flux transfrontières de données vers des destinataires situés dans des Etats n'ayant pas ratifié la Convention 108. Sur la base d'un rapport d'expert (http://www.coe.fr/dataprotection), il devrait élaborer une série de recommandations qui pourraient être adoptées lors de sa 17ème réunion.

- Projet de protocole sur la génétique humaine

Un groupe de travail du Conseil de l'Europe travaille actuellement à l'élaboration d'un protocole sur la génétique humaine. Ce protocole devrait permettre d'interdire toute discrimination d'une personne en raison de son patrimoine génétique. Durant l'année écoulée, les discussions ont porté essentiellement sur les dispositions générales du protocole, en particulier son domaine d'application, ainsi que sur le conseil génétique. Le consentement portant sur l'utilisation d'informations génétiques a également été abordé.

Le groupe de travail a pour tâche d'élaborer un protocole additionnel à la Convention du Conseil de l'Europe sur les droits de l'homme et la biomédecine (Convention d'Oviedo). La quatrième et la cinquième réunion du groupe de travail ont eu lieu du 5 au 7 avril et du 17 au 19 octobre 2000.

Le domaine d'application du protocole ne portera pas seulement sur la santé, mais aussi sur l'emploi et les assurances. Pour ce qui concerne la structure proprement dite du protocole, nous renvoyons à notre dernier rapport d'activités (cf. 7ème rapport d'activités 1999/2000, page 220ss). Les discussions n'ont pas encore porté sur l'utilisation des données génétiques dans le domaine de l'emploi et des assurances, ni sur l'ampleur de cette utilisation. A ce propos, nous estimons qu'il convient en principe d'interdire le traitement des données génétiques en matière d'emploi et d'assurances car ce sont justement deux domaines où l'on ne peut exclure une discrimination sur la base du patrimoine génétique.

En matière de conseil génétique, la personne concernée doit être informée à l'avance et de manière complète sur l'utilisation qui sera faite de ses données génétiques. Il s'agit notamment d'informations sur l'objectif, le genre et la portée des analyses génétiques. Les risques éventuellement liés à ces analyses doivent aussi être portés à la connaissance de la personne concernée. Par ailleurs, le droit de ne rien savoir fait également partie du droit à l'autodétermination individuelle en matière d'information. Ce ne sont là que quelques critères à respecter dans le domaine du conseil génétique. L'information complète de la personne concernée est également nécessaire pour que celle-ci puisse percevoir la portée de son consentement. De plus, le consentement donné à l'utilisation de

ses propres données génétiques doit être libre et révocable en tout temps. Reste à savoir si l'on pourra un jour garantir, pour la personne concernée, la transparence du traitement des analyses génétiques et surtout de ses conséquences.

Le groupe de travail s'est également penché sur les analyses génétiques systématiquement proposées (analyses en série), sur la recherche et sur la thérapie génétique.

2. Relations avec l'Union européenne

- Niveau de protection des données adéquat reconnu à la Suisse

Dans une décision du 26 juillet 2000 (voir annexe, page 235), la Commission des Communautés européennes a constaté le caractère adéquat de la protection des données personnelles en Suisse (voir aussi, 7ème rapport d'activités 1999/2000, page 222).

3. Conférence internationale des commissaires à la protection des données

La XXIIe Conférence internationale des commissaires à la protection des données s'est déroulée à Venise, du 28 au 30 septembre 2000. Elle réunissait les commissaires à la protection des données de 25 Etats du monde entier, des experts gouvernementaux, des représentants d'organisations internationales, de l'industrie, de l'informatique, de la recherche et de la science. La Conférence a adopté une déclaration réaffirmant la nécessité de principes et de standards communs en matière de protection des données eu égard à l'importance croissante des technologies dans le traitement des données, l'augmentation des utilisateurs de ces technologies et l'intensification des échanges d'informations au niveau universel. La Conférence a également fait part de sa préoccupation quant à l'insuffisance des dispositions de protection des données dans le projet de convention du Conseil de l'Europe sur la criminalité dans le cyberespace.

La Conférence a mis l'accent sur la nécessité de l'universalité de la protection de la vie privée dans un environnement global «One World, One Privacy» (www.garanteprivacy.it). Elle a examiné l'opportunité d'envisager une convention universelle sur la protection des données. Dans ce cadre, il a été rappelé

que les principes fondamentaux de la Convention 108 avaient vocation à l'universalité et qu'en particulier cette convention était ouverte à l'adhésion d'Etats non membres du Conseil de l'Europe. Elle s'est en particulier interrogée sur les risques et les avantages des technologies de l'information et a pu, sur la base de projets concrets, évaluer les progrès réalisés dans le secteur des technologies de la vie privée. Au travers de différents ateliers, les experts se sont penchés sur les avantages et les limites des clauses contractuelles dans le cadre des flux transfrontières de données. Ils ont également parlé des données génétiques, de la vidéosurveillance, des cartes à puce et des services globaux. Ils ont abordé la question de la protection de la vie privée et des médias et celle de la transparence électronique. Ils ont examiné le problème de la protection des données dans le domaine de la coopération judiciaire et policière. Enfin, la conférence s'est préoccupée de la banalisation de la vie privée, notamment du fait de certaines émissions de télévision du type «Big Brother» qui nuisent au concept même du droit à la vie privée. Cette tendance rend difficile le respect du droit à la vie privée face à une société exhibitionniste.

4. Conférence européenne des commissaires à la protection des données

Les commissaires européens à la protection des données ont tenu leur Conférence de printemps à Stockholm, les 6 et 7 avril 2000. Nous y avons pris part en tant qu'observateur. La Conférence a adopté une déclaration sur l'enregistrement des données relatives au trafic par les fournisseurs de services d'Internet. Elle a fait part de sa préoccupation face au risque d'un enregistrement et d'une conservation systématique des données de trafic pour des finalités autres que la facturation, notamment pour permettre aux autorités de poursuite pénale d'y avoir accès. Elle rappelle qu'une telle conservation est une atteinte aux droits fondamentaux, que celle-ci doit répondre à un besoin manifeste et que l'utilisation de ces données doit être régie par la loi. La durée de conservation doit être aussi courte que possible.

La Conférence a examiné la question du traitement des données génétiques et des données médicales à la lumière des expériences nationales. En Allemagne par exemple, un nouveau système de santé a été mis en place. Il règle le flux d'informations entre les établissements de soins et les caisses d'assurance. Dans ce système, on utilise des pseudonymes en lieu et place des données d'identité. L'identité exacte d'un assuré ne peut ainsi être révélée sans l'intervention d'un «trustcenter». La Conférence a ensuite débattu de la surveillance par les autorités de contrôle nationales et des procédures de plainte. Elle a également pris connaissance d'enquêtes menées conjointement par l'Espagne et les Pays-Bas auprès des fournisseurs de services Internet, ainsi que d'une étude présentée par

la France portant sur les politiques de vie privée des fournisseurs de services spécialisés dans le commerce électronique. Il est apparu nécessaire de renforcer la coopération entre autorités nationales de protection des données et notamment de développer des standards pour mener les contrôles et d'encourager les échanges entre autorités de contrôle. La Conférence s'est interrogée sur la question du droit applicable en cas de conflit dans le cadre de traitements de données personnelles effectués sur Internet. Une approche européenne intégrée sur la protection des données en ligne devrait être mise en place (voir à ce propos http://europa.eu.int/comm/internal_market/fr/media/dataprot/wpdocs/index.htm). Il est ainsi important de s'engager en faveur d'une conception des matériels informatiques et des logiciels dont l'utilisation soit compatible avec les exigences de la protection des données. La France a ainsi proposé la mise en place d'un label de protection des données européen qui pourrait être accordé à l'ensemble des sites s'engageant à informer les internautes de leurs droits et à mettre en œuvre les garanties reconnues par la directive européenne. Une autorité européenne de contrôle de qualité des différents labels délivrés par des organisations professionnelles pourrait être créée (voir également page 144). La Conférence a finalement fait le point sur l'état de la transposition de la directive européenne dans les différents Etats membres. Le représentant de la Commission européenne a en particulier relevé l'importance de l'objectif d'harmonisation et rappelé que la directive prévoit des conditions claires qui ne laissent qu'une latitude limitée aux législations nationales. La Commission évalue la situation pour vérifier si l'objectif de la libre circulation entre les Etats membres a été atteint et si des différences demeurent entre les législations nationales.

5. OCDE

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

Au cours de l'année écoulée, le groupe de travail a finalisé la mise au point du générateur permettant l'établissement automatique de déclarations de traitement de données sur Internet. Parallèlement, il a consacré ses activités à une amélioration de la protection de la sphère privé sur Internet et a entrepris de mettre à jour les inventaires des procédures d'authentification et de cryptographie. Enfin, il a décidé de collaborer avec le groupe de travail sur la génétique.

Le générateur permettant d'établir automatiquement sur Internet des déclarations-types de traitement de données a été finalisé et mis à la disposition de tous les milieux intéressés par le biais d'Internet (http://cs3-hq.

oecd.org/scripts/pwv3/pwhome.htm). Un lien direct figure sur le site du PFPD à la rubrique «News and Links». Ce générateur permet aux prestataires d'établir désormais plus facilement leurs déclarations de traitement de données - en anglais «privacy policy» - sur Internet et de garantir ainsi la transparence des traitements de données concernant leurs clients (pour plus de détails sur le générateur, se reporter au 7ème rapport d'activités 1999/2000, page 225).

Conscient du fait que bon nombre d'utilisateurs et de consommateurs n'ont encore qu'une confiance limitée dans le commerce électronique, le groupe de travail a proposé des mesures concrètes à même de nourrir cette confiance. Il a ainsi été décidé d'établir un inventaire de tous les moyens techniques permettant une protection de la sphère privée sur Internet. En même temps, le groupe de travail a décidé d'organiser une conférence sur les mécanismes de règlement des conflits dans le commerce électronique. La conférence a eu lieu les 11 et 12 décembre 2000 à La Haye (pour plus de détails sur la conférence, voir page 220).

Le groupe de travail a décidé d'adapter les inventaires des procédures d'authentification et de cryptographie aux dernières connaissances en la matière. Soulignons à cet égard que le contrôle des exportations du matériel de cryptographie a été sensiblement assoupli. Les Etats-Unis et la France ont largement libéralisé le marché du matériel de cryptographie. Néanmoins, la France désire poursuivre la recherche de solutions garantissant aux autorités d'enquêtes l'accès aux documents chiffrés. Le parlement français planchera sur une loi sur la cryptographie qui réglementera l'accès des autorités d'enquêtes. Cette loi se proposerait de considérer comme indice à la charge de l'inculpé le fait que celui-ci, dans le cadre d'une procédure, refuse de livrer le texte ou la clé.

Nous suivrons avec attention l'évolution de la question afin de voir si, outre l'accès accordé au juge d'instruction - ce qui correspond à la pratique suisse -, les autorités policières disposent également d'un accès sans décision judiciaire.

Actuellement, le groupe de travail rassemble et évalue les règles de comportement, considérées comme solution de rechange aux lois visant la protection de la sphère privée, dans le but d'en analyser l'efficacité de manière plus précise. Nous avons néanmoins constaté que les règles de comportement ne constituent pas une solution de rechange aux dispositions légales si elles ne sont pas à même de protéger efficacement la sphère privée (cf. également à ce propos le 6ème rapport d'activités 1998/1999, pages 317ss). Les règles de comportement peuvent néanmoins contribuer dans certains secteurs à rendre les obligations légales plus transparentes.

L'importance du traitement des données génétiques en relation avec la protection de la sphère privée a été reconnue. Le groupe de travail a donc décidé de se

consacrer intensément à ce thème et de collaborer à ce propos avec le groupe de travail compétent.

- Mécanismes parallèles de règlement des conflits dans le domaine des transactions en ligne, Conférence de La Haye

Les 11 et 12 décembre 2000, La Haye a accueilli une conférence de l'OCDE consacrée aux processus de règlement des conflits entre les entreprises et les consommateurs dans le domaine des transactions en ligne. Divers modèles visant le règlement des conflits et des litiges dans les échanges électroniques mondiaux ont été présentés au cours de la conférence. La nécessité d'élaborer des critères communs garant de l'efficacité au niveau mondial a également été reconnue. Il convient dans ce but de mettre en place une politique commune qui permettra d'accroître la confiance des consommateurs dans le commerce électronique grâce à un règlement efficace et juste des litiges.

Actuellement, l'efficacité des lois et des réglementations nationales relatives au règlement des conflits dans les transactions en ligne s'arrêtent généralement aux frontières nationales. Il nous faut donc trouver des solutions offrant une efficacité globale, donc internationale. Il est reconnu que les transactions du commerce électronique ne suscitent pas encore assez la confiance des consommateurs notamment parce qu'il n'existe pas de systèmes globaux permettant le règlement des conflits au niveau international. La protection de la sphère privée se heurte également aux mêmes difficultés car là aussi, il manque dans une large mesure des critères applicables au niveau international, notamment pour le règlement de conflits en cas d'atteintes à la sphère privée. En outre, la multiplication rapide des règles de comportement dans le domaine du commerce électronique est une source de confusion et influe par conséquent aussi sur la confiance des consommateurs.

Si l'on veut accroître au niveau mondial la confiance des consommateurs dans le commerce électronique, il importe de mettre en place des mécanismes permettant de régler les conflits tout en tenant compte des différences culturelles et des besoins des consommateurs. Nous devons également prendre en considération les différents systèmes juridiques. Nous ne pourrons toutefois pas réduire au même dénominateur commun mondial les différents systèmes et cultures juridiques. Il est donc d'autant plus important de jeter aujourd’hui des ponts entre les différents systèmes pour que consommateurs et entrepreneurs, comme dans les transactions commerciales traditionnelles, puissent régler leurs conflits de manière appropriée et efficace.

Un autre aspect important, que l'on néglige néanmoins souvent, est la langue utilisée. La barrière linguistique ne doit pas réduire à néant l'efficacité des mécanismes parallèles de règlement des conflits. C'est pourquoi il faut garantir que les consommateurs puissent se plaindre dans leur langue. Outre l'aspect linguistique, les valeurs et particularités culturelles doivent être prises en considération. Enfin, les entreprises aussi doivent offrir sur Internet des mécanismes de règlement des conflits en ligne qui informent les consommateurs des conditions à respecter et de l'application des mécanismes en question.

Les critères suivants doivent être remplis pour que les mécanismes parallèles de règlement en ligne des litiges puissent être efficaces:

- Examen et évaluation de tous les moyens actuels de règlement des litiges
- Fixation de critères internationaux communs pour régler des litiges en ligne
- Transparence des procédés
- Facilité d'accès aux systèmes pour les consommateurs
- Prise en compte des différences culturelles et linguistiques
- Garantie de l'indépendance lors de l'examen des cas de litige
- La voie de recours ordinaire doit demeurer ouverte pour les parties en cause.

A l'avenir, toute entreprise qui offre des prestations sur Internet devra aussi offrir des possibilités extrajudiciaires de règlement en ligne des conflits. Le consommateur devra en être informé de manière claire et compréhensible. A cet égard, la solution de la question linguistique revêtira une importance décisive.

Il est évident que ces possibilités parallèles de régler les conflits en ligne ne remplaceront pas les règles juridiques existantes. Elles ne constitueront qu'une solution de remplacement en ce sens qu'elles permettront de ne pas emprunter la voie juridique. Les représentants des milieux économiques américains sont d'un autre avis: ils voudraient, grâce à ces autres moyens de règlement, exclure totalement la voie judiciaire normale. Mais, au niveau international, cela ne contribuerait pas à accroître la confiance des consommateurs dans le commerce électronique.

La commission de l'UE a annoncé qu'elle allait édicter prochainement des critères de reconnaissance applicables à ces autres moyens de règlement en ligne des conflits, le but étant d'éviter dans la mesure du possible la longue voie procédurale ordinaire. D'ici trois ou quatre ans, l'UE désire par ailleurs mettre au point un logiciel intitulé «Intelligent agents», qui constituerait une autre solution permettant à la fois de protéger la sphère privée et de régler les conflits par un autre biais.

Quoi qu'il en soit, il ne faut pas perdre de vue qu'en cas de conflit dans le monde des affaires, le contact humain revêt encore et toujours une importance non négligeable.

6. Le principe du safe harbor – un premier pas vers la protection de la sphère privée aux Etats-Unis

En juillet 2000, au terme de deux bonnes années de négociations, l'Union européenne et les Etats-Unis sont parvenus à un accord de principe sur des normes communes en vue de la protection de la sphère privée. Cet accord devra permettre l'échange d'informations au niveau international, facilitant ainsi le commerce électronique. Bien que ce même accord prévoit l'application obligatoire d'un certain nombre de règles importantes visant la protection de la sphère privée (comme le droit d'être informé et le droit de s'opposer au traitement), il faudra encore attendre pour voir si l'accord en question aura l'efficacité que l'on en attend.

En adhérant au principe du safe harbor, les entreprises américaines s'engagent à respecter un certain nombre d'exigences européennes en matière de protection des données. Néanmoins, elles sont libres «d'entrer» dans ce safe harbor; en d'autres termes, ses principes ne sont applicables qu'aux entreprises américaines qui se sont inscrites sur la liste publique établie à cet effet par le ministère américain du commerce (cf. http://export.gov/safeharbor/). Les entreprises qui y figurent contractent des engagements légaux. Le ministère américain du commerce surveille le respect des principes ainsi posés et des conséquences juridiques sont prévues pour les entreprises qui ont failli à leurs engagements.

Les consommateurs européens ont le droit d'être informés par une entreprise qui s'est engagée à respecter les principes du safe harbor si leurs données personnelles sont transmises et à qui, ce qui équivaut au droit d'accès européen. En outre, les données sensibles ne peuvent être transmises à des tiers qu'avec le consentement exprès des personnes concernées. Il est prévu que le ministère américain du commerce contrôle une fois par an le respect de ces règles.

Bien que l'adoption des principes du safe harbor constitue un premier pas dans la bonne direction, il faut encore attendre pour voir s'ils permettent de protéger efficacement la sphère privée. Il convient en particulier de souligner le fait que ces principes ne répondent pas à toutes les exigences légales européennes et ne tiennent compte que des principes de base comme l'information et le consentement de la personne concernée. En outre, les principes du safe harbor ne sont

pas des dispositions contraignantes. Les entreprises s'y soumettent volontairement. Jusqu'ici (état janvier 2001), une douzaine d'entreprises seulement se sont inscrites sur la liste en question, de sorte que les principes du safe harbor ne produisent aucun effet sur la majorité des entreprises américaines.

Nous recommandons donc aux entreprises transmettant des données personnelles vers les Etats-Unis de continuer à veiller à la protection des données transmises en signant des contrats individuels.

7. La Convention EUROPOL

Dans le cadre d'échanges de vue sur les conditions de négociation visant à la conclusion d'accords de coopération entre Europol et certains Etats tiers, l'Office fédéral de la police a organisé la visite à Berne de deux représentants d'Europol. Invités à participer à cette rencontre, nous avons exposé la situation de la législation et de la pratique suisse en matière de protection des donnée et mis en évidence les aspects de protection des données devant encore être examinés dans l'optique de futures négociations.

L'Office européen de police Europol a été institué par la Convention du même nom conclue en 1995 par les quinze Etats membres de l'Union européenne. Europol a pour objectif d'améliorer l'efficacité des services compétents des Etats membres et leur coopération en ce qui concerne notamment la prévention et la lutte contre le terrorisme, le trafic illicite de stupéfiants et d'autres formes graves de criminalité internationale. En vue de remplir ses fonctions, Europol a mis en place un système d'informations alimenté directement par les services de police des Etats membres. La Convention Europol prévoit une réglementation très stricte en ce qui concerne la gestion de ce système informatisé. De très nombreuses dispositions réglementent également la protection des données (niveau de protection, traitement des données, droit d'accès, autorités de contrôle, sécurité des données...).

Selon les informations transmises par le Bureau de l'intégration et l'Office fédéral de la police (OFP), le Conseil des ministres de l'Union européenne a adopté en mars 2000 une décision autorisant le directeur d'Europol à engager des négociations en vue de la conclusion d'accords de coopération avec certains Etats et organisations tiers. En tant que telle, cette décision ne vise à ce stade qu'un accord de type technique ou stratégique. Pour des échanges de données personnelles, un accord de type opérationnel est nécessaire. Ce dernier nécessite une procédure plus lourde comprenant notamment l'élaboration par Europol d'un rapport sur la législation et la pratique administrative en matière de protection

des données de l'Etat tiers concerné. En effet, les aspects liés à la protection des données constituent un élément déterminant dans le cadre de négociations entre Europol et des Etats tiers. Une coopération avec un Etat tiers ne peut avoir lieu, dans la mesure où elle comprend l'échange de données personnelles, que si l'Etat dispose d'une législation et d'une pratique conformes aux exigences de la Convention Europol et de la législation dérivée en matière de protection et de sécurité des données.

En août 2000, l'OFP a reçu la visite à Berne de deux représentants d'Europol chargés d'examiner la situation en Suisse et de rédiger un rapport portant notamment sur les systèmes informatiques de l'OFP et sur la protection des données. Invités à participer à cette rencontre, nous avons présenté les différentes compétences que nous attribue la loi fédérale sur la protection des données. Nous avons également pris position sur le niveau d'adéquation de la législation suisse en regard des exigences de protection des données instaurées par Europol.

Nous avons ainsi relevé que du point de vue des standards légaux à mettre en place, la Suisse répondait de manière adéquate aux exigences imposées par Europol. Peuvent notamment être cités la ratification de la Convention no 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et l'adoption de la Recommandation du Conseil de l'Europe R (87) 15 sur l'utilisation des données à caractère personnel dans le secteur de la police. Nous avons également rappelé l'existence de législations fédérale et cantonales de protection des données, la mise en place d'organes de contrôle indépendants de protection des données tant au niveau fédéral que cantonal, l'élaboration de lois au sens formel réglementant les systèmes informatiques de police ou encore la décision de la Commission de l'Union européenne reconnaissant le caractère adéquat de la législation suisse en matière de protection des données.

Nous avons par contre, en tant qu'organe de contrôle, rappelé que nous n'étions pas en mesure à ce stade de déclarer que tout est en ordre du point de vue de la protection des données dès lors que nous ne sommes pour l'instant pas en possession des détails suffisants sur les démarches entreprises ou l'état d'avancement de négociations entre l'OFP et Europol. De nombreux points pratiques devront en effet encore être examinés tels que par exemple les systèmes informatiques de polices concernés, les modalités d'exercice du droit d'accès ou la répartition des compétences des organes de contrôle de protection des données.

Nous avons demandé à l'OFP de nous informer régulièrement de la situation de ce dossier et de l'état d'avancement d'éventuelles négociations. Nous avons

d'autre part convenu avec les représentants d'Europol que nous nous tenions à leur disposition pour toute question relative à la protection des données.

8. Protection des données au Kosovo

Dans le cadre de la mission de l'OSCE au Kosovo, un collaborateur du PFPD a été détaché sur place en tant que préposé à la protection des données. La question de la sécurité des données surtout était au centre des préoccupations. Il s'agissait essentiellement d'éviter que les données personnelles des différents groupes ethniques au Kosovo tombent aux mains de personnes à qui elles n'étaient pas destinées.

Au cours de l'année écoulée, les Nations Unies et l'OSCE ont procédé à l'enregistrement de la population au Kosovo. Cette mesure s'imposait du fait qu'une partie des registres de l'état civil avaient été soit volés, soit détruits durant la guerre. C'est également sur la base de cet enregistrement de la population qu'ont été organisées les élections municipales de l'automne 2000. Le préposé à la protection des données au Kosovo a appuyé ses travaux sur les normes légales des Nations Unies ainsi que sur la Convention européenne des droits de l'Homme (CEDH).

Du point de vue du droit de la protection des données, toutes les données personnelles existant au Kosovo sont à classer comme sensibles. En effet, ne serait-ce que les noms de famille donnent des indications claires sur les groupes ethniques de la région (Albanais du Kosovo, Serbes, Turcs etc.). En d'autres termes, une liste d'adresses au Kosovo doit déjà être considérée comme un ensemble de données sensibles.

Les données concernant les minorités vivant au Kosovo qui désiraient se faire enregistrer ont dû faire l'objet d'une protection spéciale; en effet, la situation entre les différentes ethnies était, et est encore, particulièrement tendue. Dans ce contexte, des mesures techniques et organisationnelles (contrôle d'accès, contrôle des installations à l'entrée, contrôle du transport etc.) surtout ont été prises. Il s'agissait essentiellement de détecter les éventuelles lacunes en matière de sécurité durant tout le processus de l'enregistrement. Par ailleurs, le préposé à la protection des données au Kosovo a attiré l'attention des collaborateurs de l'OSCE et des Nations Unies sur la sensibilité des données.

Cet enregistrement de la population a permis de rassembler de très nombreuses données personnelles. Chaque requérant a dû en particulier donner une empreinte digitale pour éviter les doubles enregistrements. Le principe de la pro-

portionnalité exigeait également l'annulation des données personnelles qui n'étaient plus nécessaires au but de l'enregistrement. Il n'a malheureusement pas été respecté partout.

Durant la campagne électorale, l'accent a été mis en particulier sur la protection des données concernant les membres des minorités ethniques qui désiraient prendre part aux élections communales. Certaines personnes avaient en effet peur de voter dans une localité déterminée. Il a donc fallu mettre en place des mesures leur permettant de voter à domicile.

Enfin, un projet de loi sur la protection des données pour l'ensemble du Kosovo a été élaboré. Ce projet renferme les normes essentielles de protection des données en vigueur en Europe et concerne tous les traitements de données effectués par l'administration au Kosovo. Le Kosovo a en effet absolument besoin d'une loi qui protège les droits de la personnalité de ses habitants. Il faut espérer que ce projet aura une suite.

IV. PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES

1. Les publications du PFPD - Nouvelles parutions

- Guide relatif à la surveillance d'Internet et du E-Mail sur le lieu de travail

- Schéma sur les conditions et le déroulement correct de la surveillance d'Internet et du E-Mail sur le lieu de travail

- Aide mémoire sur la vidéosurveillance effectuée par des personnes privées

Vous trouverez le schéma et l' aide-mémoire en annexe du présent rapport (voir pages 239 et 240). Ils peuvent également être consultées sur notre site Web (www.edsb.ch).

- Feuille d'information du PFPD 2/2000
- Feuille d'information du PFPD 1/2001

Les feuilles d'information peuvent être consultées sur notre site Web (www.edsb.ch).

2. Statistique des activités du Préposé fédéral à la protection des données Période du 1er avril 2000 au 31 mars 2001

Participations à des conférences

Nationales	Internationales
25	18

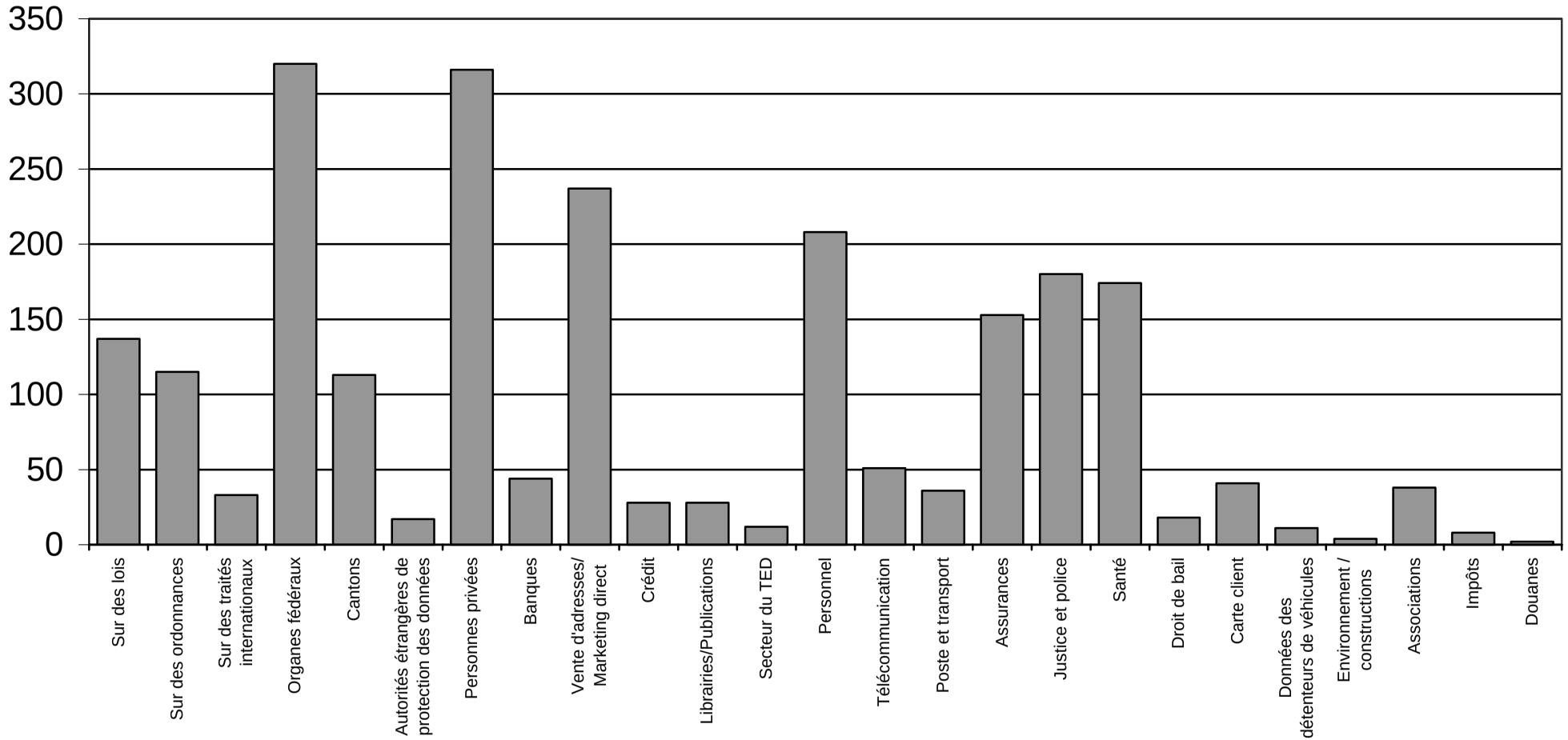
Nombre de séances

	Confédération	Personnes privées	Cantons
A l'intérieur	293	115	19
A l'extérieur	143	75	29
Total	436	190	48

Nombre de prises de position

	Entrées	Prises de position écrites	Recommandat-ions du PFPD	Pas d'objections
Sur des lois	67	61		9
Sur des ordonnances	52	42		21
Sur des traités internationaux	18	9		6
Questions du secteur public:				
Organes fédéraux	180	136		4
Cantons	61	52		
Autorités étrangères de protection des données	10	7		
Questions du secteur privé:				
Personnes privées	181	133	2	
Banques	22	19		3
Vente d'adresses / Marketing direct	129	108		
Crédit	16	12		
Librairies/Publications	15	13		
Secteur du TED	6	6		
Personnel	4	204		
Télécommunication	49	2		
Poste et transport	18	18		
Assurances	82	71		
Justice et police	91	88	1	
Santé	94	80		
Droit de bail	9	9		
Carte client	21	20		
Données des détenteurs de véhicules	5	5	1	
Environnement / constructions	2	2		
Associations	22	16		
Impôts	4	4		
Douanes	1	1		
Total	1159	1118	4	43

Nombre de prises de position

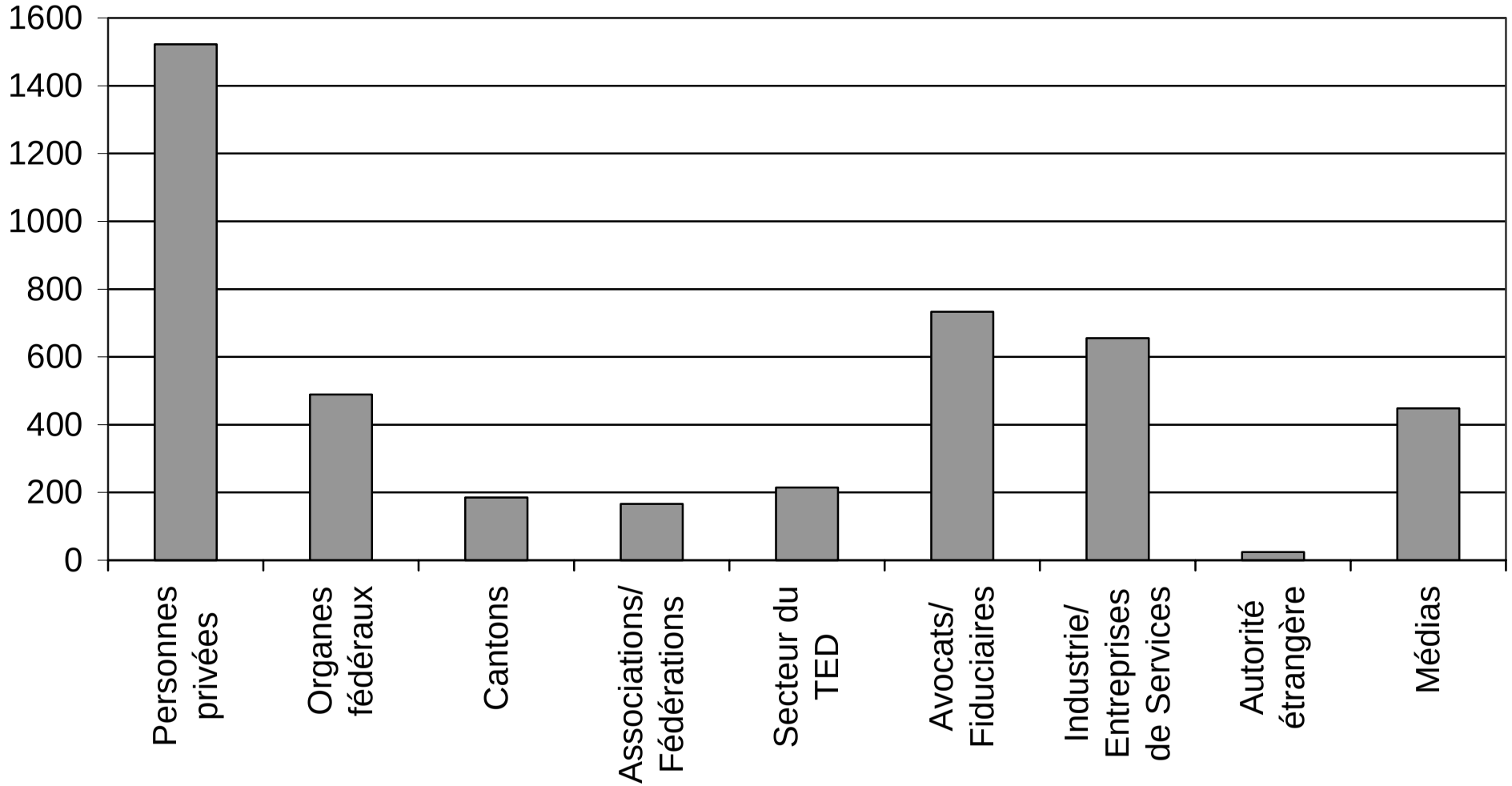


RENSEIGNEMENTS PAR TELEPHONE

	Personnes privées	Organes fédéraux	Cantons	Associa-tions / Fédérations	Secteur du TED	Avocats / Fiduciaires	Industrie / Entreprises de Services	Autorité étrangère	Médias
Protection des données en général	218	151	38	20	10	131	61	1	68
Droit d'accès	108	22	10	21		8	1		7
Annonce de fichiers	62	16	1	8		47	11		
Communication de données	86	19	5	30	5	81	107		42
Flux à l'étranger	59			7	25	118	61	1	10
Compatibilité avec les pays de l'UE	15	12	4	3	19	57	52	1	21
Secteur du travail/ Placement	237	36	16	1	39	96	154	12	53
Santé/Assurances	307	97	47	2	43	63	16	1	15
Droit de bail Formulaires	12			1					
Marketing direct/Publicité	53	2		23	9	8	19	1	29
Banques/ Crédits Renseignements	71	2		7		24	22		33
Statistiques	32	18	30			1	11	3	34
Registre de véhicules	3		1					1	2
Surveillance vidéo	30	7	6		10	3	12	1	37
Téléphone IRNS/ Données Telecom	63	3	2	10	4	36	30	2	21
INTERNET	79	15	7	16	8	19	37		30
Sécurité des données/Cryptographie	30	29	6	9	25	10	23		14
Affaires de police	40	23	11			6			6
Douanes	1	7	1						
Asile / Étrangers	3	18		7					1
Impôts	4								
Militaire	5	3							
E-Commerce	2	1		1	18	25	38		10
DNA génétique	2	8							15
Total	1522	489	185	166	215	733	655	24	448

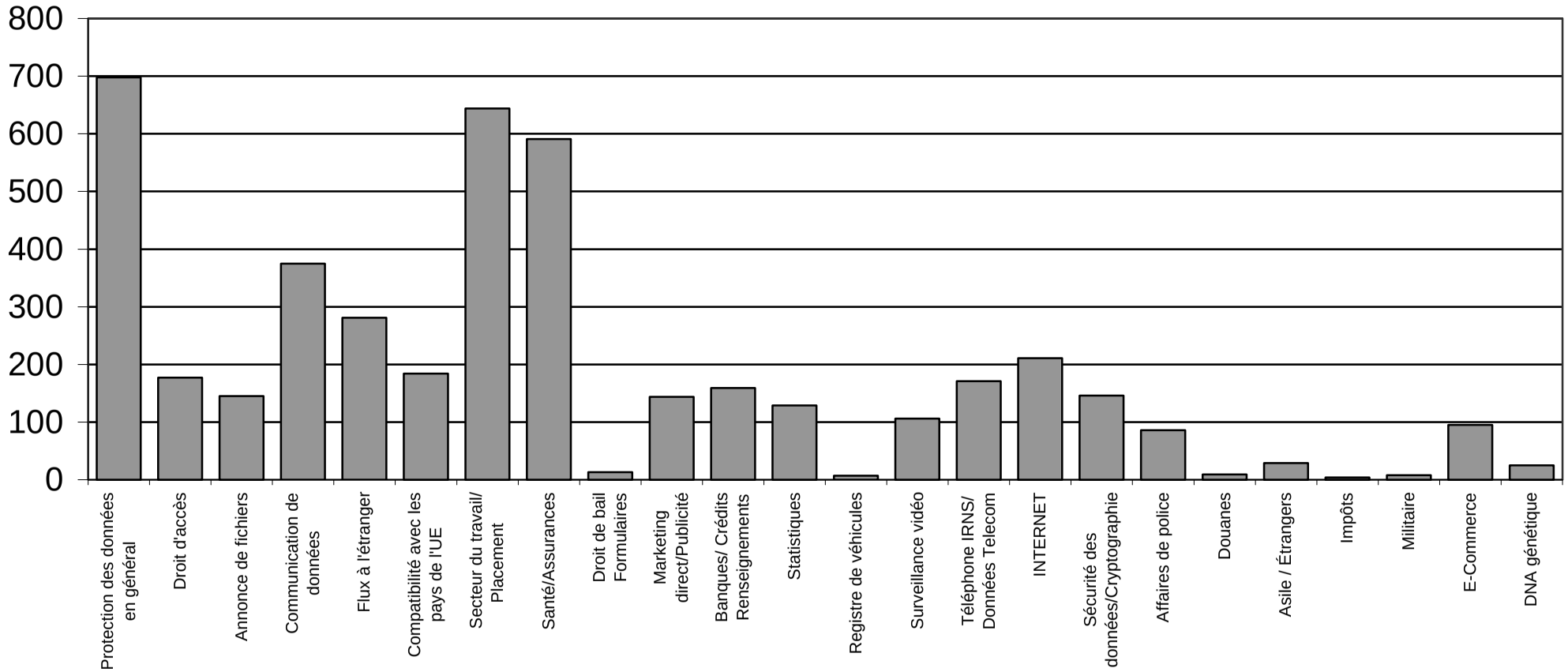
Renseignements par téléphone

selon la provenance des appels



Renseignements par téléphone

par matière



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

Préposé fédéral à la protection des données:	**Guntern Odilo, dr en droit**
Suppléant:	Walter Jean-Philippe, dr en droit
Secrétariat:	
Chef:	Walter Jean-Philippe, dr en droit
Suppléant:	Buntschu Marc, lic. en droit
Service d'information et de presse:	Eggli Liliane, lic. phil. Tsiraktsopulos Kosmas, lic. en droit
Service juridique:	8 personnes
Service informatique:	3 personnes
Chancellerie:	3 personnes

V. ANNEXES

1. Décision de la Commission de l'UE concernant le caractère adéquat de la protection des données en Suisse

II

(Actes dont la publication n'est pas une condition de leur applicabilité)

COMMISSION

DÉCISION DE LA COMMISSION

du 26 juillet 2000

relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse

(notifiée sous le numéro C(2000) 2304)

(Texte présentant de l'intérêt pour l'EEE)

(2000/518/CE)

LA COMMISSION DES COMMUNAUTÉS EUROPÉENNES, —

vu le traité instituant la Communauté européenne, vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [1], et notamment son article 25, paragraphe 6,

considérant ce qui suit:

(1) Conformément à la directive 95/46/CE, les États membres sont tenus de veiller à ce que les transferts de données à caractère personnel vers un pays tiers n'aient lieu que si le pays tiers en question assure un niveau de protection adéquat et si les lois des États membres qui mettent en œuvre d'autres dispositions de la directive sont respectées avant le transfert.

(2) La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat. Dans ce sens, des données à caractère personnel peuvent être transférées à partir des États membres, sans qu'aucune garantie supplémentaire ne soit nécessaire.

(3) Conformément à la directive 95/46/CE, le niveau de protection des données à caractère personnel doit être apprécié au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données et compte tenu de conditions déterminées. Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par ladite directive a donné des indications sur ces évaluations [2].

(4) Compte tenu des différentes approches retenues par les pays tiers en matière de protection des données à caractère personnel, il convient de faire en sorte que l'évaluation du caractère adéquat de cette protection et l'application de toute décision au titre de l'article 25, paragraphe 6, de la

[1] JO L 281 du 23.11.1995, p. 31.

[2] Avis 12/98, adopté par le groupe le 24 juillet 1998: «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données» (DG MARKT D/5025/98), disponible sur le site Web «Europa» de la Commission Š http://europa.eu.int/comm/internal_market/en/ media/dataprot/wpdocs/index.htm

directive 95/46/CE ne créent pas de discrimination arbitraire ou injustifiée à l'égard de pays tiers où des conditions similaires existent ou entre les pays tiers, et ne constituent pas une entrave déguisée aux échanges eu égard aux engagements internationaux actuels de la Communauté.

(5) La Confédération suisse dispose, en matière de protection des données à caractère personnel, de normes produisant des effets juridiques contraignants tant au niveau fédéral que cantonal.

(6) La constitution fédérale, modifiée par votation populaire le 18 avril 1999 et entrée en vigueur le 1er janvier 2000, donne à toute personne le droit au respect de sa vie privée et, en particulier, le droit d'être protégée contre l'emploi abusif des données qui la concernent. Sur la base de la constitution antérieure, qui ne contenait pas une telle disposition, le Tribunal fédéral a développé une jurisprudence fixant les principes généraux applicables aux traitements de données à caractère personnel en ce qui concerne notamment la qualité des données traitées, le droit d'accès des personnes concernées et le droit de demander la rectification ou la destruction des données. Ces principes sont contraignants tant au niveau fédéral que cantonal.

(7) La loi suisse sur la protection des données du 19 juin 1992 est entrée en vigueur le 1er juillet 1993. Les modalités d'application de certaines dispositions de la loi en ce qui concerne notamment le droit d'accès des personnes concernées, la déclaration des traitements à l'autorité de contrôle indépendante ou la communication de données à l'étranger, ont été fixées par ordonnances du Conseil fédéral. La loi s'applique aux traitements de données à caractère personnel effectués par les organes fédéraux et par l'ensemble du secteur privé, ainsi qu'aux traitements effectués par les organes cantonaux en exécution du droit fédéral, dans la mesure où ces traitements ne font pas l'objet de dispositions cantonales sur la protection des données.

(8) La plupart des cantons ont adopté une législation en matière de protection des données pour les domaines relevant de leurs compétences, lesquels concernent en particulier les hôpitaux publics, l'éducation, les impôts cantonaux directs et la police. Dans les autres cantons, les traitements sont régis par des actes de nature réglementaire ou par les principes de la jurisprudence cantonale. Quels que soient la source et le contenu des dispositions cantonales ou même en l'absence de dispositions cantonales, les principes constitutionnels doivent être respectés par les cantons. Dans leur domaine de compétence, les autorités cantonales peuvent être amenées à transférer des données à caractère personnel à des administrations publiques d'États limitrophes, principalement à des fins d'assistance mutuelle pour la sauvegarde d'intérêts publics importants ou, s'agissant des hôpitaux publics, en vue de protéger les intérêts essentiels des personnes concernées.

(9) 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 des données à caractère personnel (convention n o 108) [3] qui vise à renforcer la protection des données à caractère personnel et à assurer la libre circulation entre les parties contractantes, sous réserve de dérogations que celles-ci peuvent prévoir. Sans être directement applicable, la convention fixe des engagements internationaux aussi bien à l'égard de la fédération que des cantons. Ces engagements concernent non seulement les principes fondamentaux de la protection auxquels chaque partie contractante doit donner effet dans son droit interne, mais aussi les mécanismes de coopération entre les parties contractantes. En particulier, les autorités suisses compétentes doivent fournir aux autorités des autres parties contractantes qui en font la demande toute information sur le droit et la pratique administrative en matière de protection des données, ainsi que les informations concernant un traitement automatisé déterminé. Elles doivent également prêter assistance à toute personne résidant à l'étranger pour l'exercice de son droit d'être informée de l'existence de traitements de données la concernant, d'accéder aux données la concernant, d'en demander la rectification ou la destruction, et de disposer de voies de recours.

(10) Les normes applicables en Suisse englobent tous les principes fondamentaux nécessaires pour constater un niveau de protection adéquat des personnes physiques, même si des dérogations et des limitations sont également prévues pour la sauvegarde d'intérêts publics importants. L'application de ces normes est garantie par les recours juridictionnels et par le contrôle

[3] http://conventions.coe.int/treaty/EN/cadreintro.htm

indépendant exercé par les autorités, notamment par le préposé fédéral doté de pouvoirs d'investigation et d'intervention. Par ailleurs, les dis- positions du droit suisse relatives à la responsabilité civile s'appliquent en cas de traitement illicite portant préjudice aux personnes concernées.

(11) Dans un souci de transparence et en vue de permettre aux autorités compétentes des États membres d'assurer la protection des individus en ce qui concerne le traitement des données à caractère personnel, il est nécessaire d'indiquer dans la présente décision dans quelles circonstances exceptionnelles la suspension de certains flux de données peut être justifiée, même lorsque le niveau de protection assuré a été jugé adéquat.

(12) Le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué à l'article 29 de la directive 95/46/CE a rendu un avis [4] sur le niveau de protection assuré par la législation suisse; il en a été tenu compte lors de l'élaboration de la présente décision.

(13) Les mesures prises par la présente décision sont conformes à l'avis du comité institué à l'article 31 de la directive 95/46/CE,

A ARRÊTÉ LA PRÉSENTE DÉCISION:

Article premier

Aux fins de l'article 25, paragraphe 2, de la directive 95/46/CE, la Suisse est considérée comme offrant un niveau de protection adéquat des données à caractère personnel transférées à partir de la Communauté pour toutes les activités entrant dans le champ d'application de ladite directive.

Article 2

La présente décision concerne uniquement le caractère adéquat de la protection assurée en Suisse en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive 95/46/CE et n'affecte pas l'application d'autres conditions ou restrictions transposant d'autres dispositions de ladite directive qui se rapportent au traitement de données à caractère personnel dans les États membres.

Article 3

(1) Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les transferts de données à un destinataire situé en Suisse afin de protéger les personnes en ce qui concerne le traitement de leurs données à caractère personnel dans les cas suivants:

a) lorsqu'une autorité suisse compétente a constaté que le destinataire ne respecte pas les normes applicables en matière de protection ou
b) lorsqu'il est très probable que les normes de protection n'ont pas été respectées, qu'il y a tout lieu de croire que l'autorité suisse compétente ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent pour régler l'affaire en question, que la poursuite du transfert entraînerait un risque imminent de grave préjudice pour les personnes concernées et que les autorités compétentes de l'État membre se sont raisonnablement efforcées dans ces circonstances d'avertir le responsable du traitement établi en Suisse et de lui donner la possibilité de répondre.

La suspension cesse dès que le respect des normes de protection est assuré et que l'autorité compétente concernée dans la Communauté en est avertie.

(2) Les États membres informent sans tarder la Commission des mesures adoptées au titre du paragraphe 1.

[4] Avis no 5/99, adopté par le groupe le 7 juin 1999 (DG MARKT 5054/99), disponible sur le site Web «Europa» de la Commission indiqué à la note 2 de bas de page.

(3) Les États membres et la Commission s'informent muellement des cas dans lesquels les mesures prises par les organismes chargés de veiller au respect des normes de protection en Suisse ne suffisent pas à assurer ce respect.

(4) Si les informations collectées en application des paragraphes 1, 2 et 3 montrent qu'un organisme chargé de faire respecter les normes de protection en Suisse ne remplit pas efficacement sa mission, la Commission en informe l'autorité suisse compétente et, si nécessaire, présente un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46/CE en vue d'abroger ou de suspendre la présente décision ou d'en limiter la portée.

Article 4

(1) La présente décision peut être adaptée à tout moment à la lumière de l'expérience tirée de son application ou en cas de modification de la législation suisse. La Commission évalue, sur la base des informations disponibles, la mise en œuvre de la présente décision trois ans après sa notification aux États membres et communique au comité institué à l'article 31 de la directive 95/46/CE toute constatation pertinente, et notamment tout élément susceptible d'avoir une incidence sur l'évaluation faite à l'article 1er de la présente décision du niveau de protection adéquat assuré en Suisse au sens de l'article 25 de la directive 95/46/CE et tout élément montrant que la présente décision est appliquée de façon discriminatoire.

(2) La Commission présente, si nécessaire, un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46/CE.

Article 5

Les États membres prennent toutes les mesures nécessaires pour se conformer à la présente décision au plus tard quatre-vingt-dix jours après la date de sa notification aux États membres.

Article 6

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 26 juillet 2000.

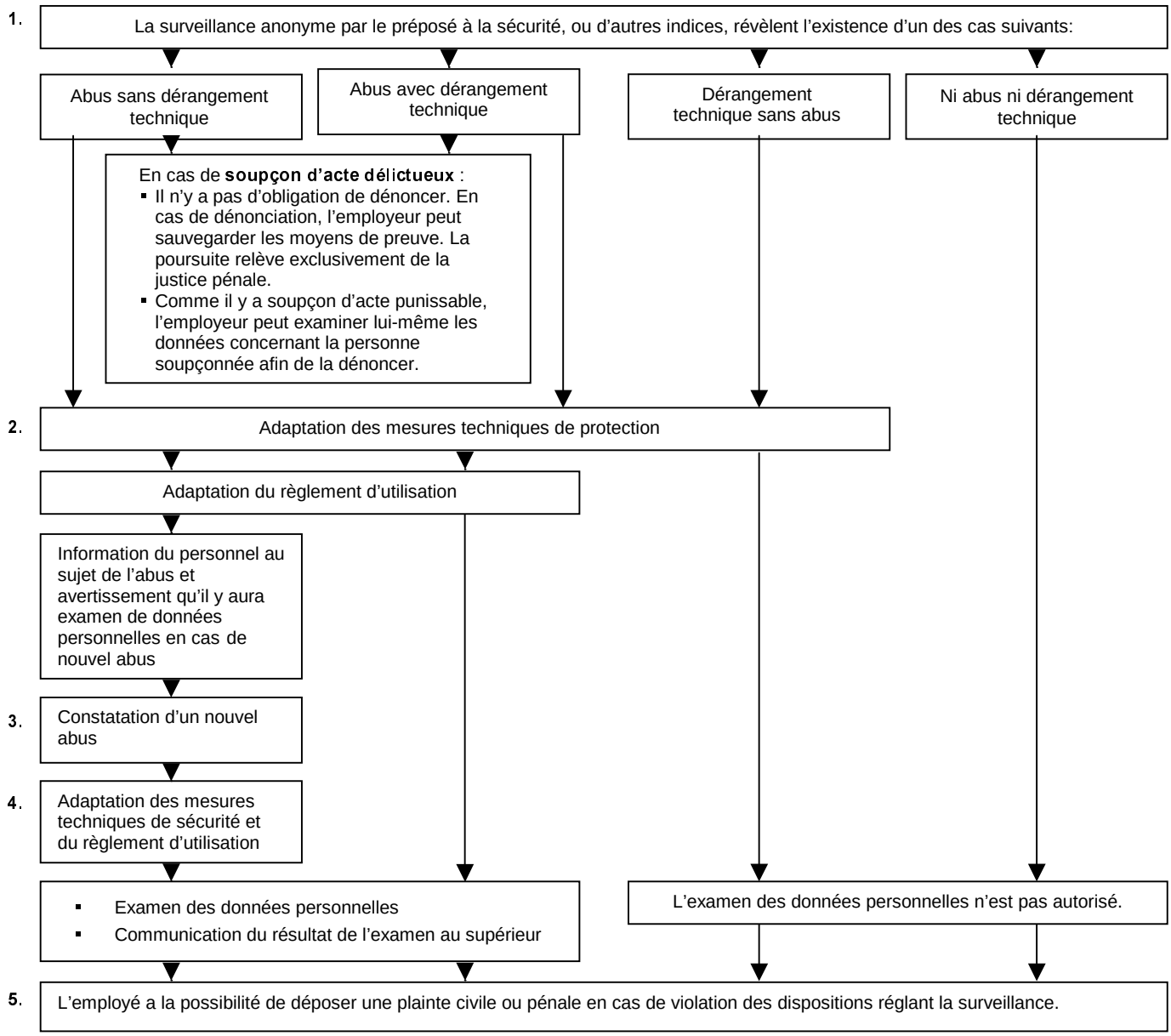
Par la Commission
Frederik BOLKESTEIN
Membre de la Commission

2. Schéma de surveillance de l'Internet et du E-Mail sur le lieu de travail

A. CONDITIONS D'EXERCICE DE LA SURVEILLANCE

1. L'employeur applique des mesures techniques de protection telles que programmes antivirus, pare-feu (firewall), limites d'utilisation du disque, copies de sauvegarde. L'utilisation de programmes de surveillance (mouchards) est interdite. L'employeur détermine les activités qui doivent faire l'objet d'un fichier journal et fait en sorte que seul le préposé à la sécurité y ait accès en cas de besoin.
2. L'employeur porte à la connaissance du personnel :
   - les **mesures techniques de protection** prises et le fait qu'un fichier journal est tenu pour certaines activités
   - le **règlement d'utilisation**
     Le règlement d'utilisation est un document écrit qui détermine si l'usage d'Internet et de la messagerie électronique est autorisé et à quelles conditions. Un tel règlement est recommandé car il clarifie la situation.
   - les mesures de **surveillance**
     Les préposés à la sécurité procèdent en permanence à des surveillances anonymes des ressources techniques (Intrusion and Abuse Detection) et sont en mesure de vérifier de façon anonyme le respect des règlements d'utilisation au moyen de contrôles ponctuels. Ce n'est qu'après qu'un indice d'abus a été constaté que l'employeur peut procéder au contrôle du fichier journal personnel. Il y a abus lorsqu'il y a violation du règlement d'utilisation ou du devoir de loyauté envers l'employeur. Pour pouvoir contrôler les données à caractère personnel, la publication d'un règlement relatif à la surveillance est indispensable. Ce règlement régit aussi la communication des résultats des contrôles aux supérieurs hiérarchiques et la prise de sanctions.
     N.B. - La surveillance du courrier électronique est, pour des raisons techniques, toujours à caractère personnel et ne peut porter que sur les indications de confidentialité (privé, personnel, confidentiel) ou les éléments d'adressage. En cas de doute sur le caractère privé ou non des messages, il y a lieu d'interroger la personne concernée.
     - Les fichiers journaux relatifs aux activités que les mesures techniques de protection visent à prévenir ne peuvent être examinés que de manière anonyme.

B. DEROULEMENT DE LA SURVEILLANCE



3. Aide mémoire sur la vidéosurveillance effectuée par des personnes privées

Le Préposé fédéral à la protection des données informe:

AIDE MEMOIRE SUR LA VIDÉOSURVEILLANCE EFFECTUÉE PAR DES PERSONNES PRIVÉES

L'utilisation de caméras vidéo à des fins de surveillance par des personnes privées est soumise à la loi fédérale du 19 juin 1992 sur la protection des données (LPD; RS 235.1) dès lors que les images filmées se rapportent à une ou plusieurs personnes identifiées ou identifiables, que les images fassent ou non l'objet d'une conservation. Les traitements effectués (capter, transférer, visionner en direct ou a posteriori, conserver des images etc.) doivent respecter les principes généraux de protection des données.

Cette feuille d'information concerne la vidéosurveillance effectuée par des personnes privées dans des lieux privés accessibles ou non au public. Elle ne concerne pas la vidéosurveillance sur le lieu de travail (vous trouverez des informations à ce sujet dans le 4ème Rapport d'activités du Préposé fédéral à la protection des données, chapitre I, titre 4.2).

Un système de vidéosurveillance n'est autorisé que si les deux conditions suivantes sont remplies:

1. La vidéosurveillance ne peut être effectuée que si cette atteinte à la personnalité est justifiée par le consentement des personnes concernées, par un intérêt prépondérant public ou privé ou par la loi. (Principe de la licéité)

   Exemple: Un bijoutier peut avoir un intérêt prépondérant à ce que son commerce ne soit pas cambriolé pendant son absence.

2. La vidéosurveillance doit être un moyen adéquat et nécessaire à la réalisation de l'objectif poursuivi, à savoir la sécurité, notamment la protection contre les atteintes aux biens et/ou aux personnes. Elle ne peut être retenue que si d'autres mesures moins attentatoires à la vie privée telles que verrouillages complémentaires, renforcement des portes d'entrée, systèmes d'alarmes, s'avèrent insuffisantes ou impraticables. (Principe de la proportionnalité)

   Exemple: L'installation de caméras vidéo dans une halle d'entreposage pour éviter des actes de vandalisme sera en règle générale admissible.

Les exigences en matière d'installation et d'utilisation d'un système de vidéo-surveillance sont énumérées au verso.

Vous trouverez d'autres informations sur la protection des données sur le site www.edsb.ch. Vous pouvez également vous adresser directement au Préposé fédéral à la protection des données, 3003 Berne, tél. 031 322 43 95, fax 031 325 99 96 ou info@edsb.ch.

En cas d'installation et d'utilisation d'un système de vidéo-surveillance, les règles suivantes doivent être respectées:

1. Le responsable du système de vidéosurveillance doit informer les personnes entrant dans le champ des caméras de surveillance de l'utilisation d'un tel système par le biais d'un avis lisible. Dans le cas où les images sont reliées à un fichier, l'avis doit également indiquer auprès de qui le droit d'accès peut être effectué si cela ne ressort pas du contexte. (Principe de la bonne foi et droit d'accès)

   Exemple: Une caméra vidéo placée à l'entrée d'un immeuble locatif devra être signalée par un panneau bien visible pour toute personne qui pénètre dans le bâtiment.

2. Le responsable du système de vidéosurveillance doit prendre les mesures organisationnelles et techniques appropriées afin de protéger les données personnelles contre tout traitement non autorisé. (Sécurité des données)

   Exemple: Seul les personnes autorisées ont accès aux écrans des caméras-vidéo. Les données enregistrées doivent être conservées en un endroit sûr et dans un local fermé à clé et seul les personnes autorsées doivent avoir accès à la clé.

3. L'installation d'une caméra doit être effectuée de façon à ce que n'entrent dans son champ que les images strictement nécessaires à la surveillance envisagée. (Principe de la proportionnalité)

   Exemple: Une caméra placée à l'entrée d'un immeuble locatif ne devra pas permettre de voir quelle personne se rend dans quel appartement.

4. Les données ne peuvent être utilisées que dans le cadre de la protection contre les atteintes aux biens et aux personnes. Elles ne peuvent donner lieu à d'autres utilisations. (Principe de la finalité)

   Exemple: Les images prises par une caméra vidéo installée dans le but d'assurer la sécurité ne pourront pas être utilisées à des fins de marketing.

5. La communication de données personnelles enregistrées par une caméra est interdite sauf dans les cas prévus ou autorisés par la loi, par exemple une demande émanant d'un juge. (Principe de la finalité)

   Exemple: Les images prises ne peuvent pas être transmises ou vendues à des tiers.

6. Les données personnelles enregistrées par une caméra doivent être effacées dans un délai particulièrement bref. En effet la constatation d'une infraction aux biens ou aux personnes aura lieu dans la plupart des cas dans les heures qui suivent sa perpétration. Un délai de 24 heures apparaît donc suffisant au regard de la finalité poursuivie dans la mesure où aucune atteinte aux biens ou aux personnes n'est constatée dans ce délai. Ce délai peut être plus long dans certains cas de vidéosurveillance de lieux privés non accessibles au public. (Principe de la proportionnalité)

   Exemple: Une absence pour cause de vacances peut justifier une durée de conservation plus longue. Dans ce cas, les images devront être détruites aussi vite que possible après le retour si aucune déprédation n'a été constatée.

4. Recommandations du PFPD

4.1. Recommandation concernant la gestion des absences

voir page 116

4.2. Recommandation concernant la réexpédition (La Poste)

voir page 119

4.3. Recommandation concernant le dépistage de drogues chez les apprentis

voir page 122