15ème Rapport d'activités 2007/2008

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2007/2008 du Préposé fédéral à la protection des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence 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 2007 au 31 mars 2008.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ce rapport est également disponible sur Internet (www.edoeb.admin.ch)

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.015.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Dans notre dernier rapport d'activités, je comparais le rôle du Préposé à la protection des données à celui de la figure tragique de la mythologie grecque qu'est Sisyphe, condamné à pousser éternellement le même rocher au sommet d'une montagne: à peine pensons-nous avoir résolu un problème touchant à la protection des données qu'un nouveau surgit! Bien que cette métaphore soit toujours d'actualité au fil des années, le rapport annuel est l'occasion de jeter un coup d'oeil rétrospectif et d'apprécier les résultats obtenus. En bref, nous pouvons dire qu'une approche pragmatique de la protection des données est porteuse de succès.

Commençons par le domaine de la santé, dans lequel les choses bougent beaucoup suite à nos recommandations dans le cas CSS. Avec notre soutien, la Société suisse des médecins-conseils a adopté en décembre 2007 des recommandations ayant pour objectif de renforcer l'indépendance des médecins-conseils vis-à-vis des assurances. La circulation des données à l'intérieur du Service du médecin-conseil a été réglementée de manière plus claire et l'indépendance administrative mieux organisée. Etant donné que les assureurs-maladies offrent des produits les plus divers comme les assurances d'indemnités journalières et les assurances-vie dans le cadre de holdings aux larges ramifications, il est nécessaire de procéder à une clarification du rôle de médecins-conseils (instauré par la LAMal) agissant également dans le cadre des assurances non obligatoires. De plus, le rôle des case managers demeure peu clair et la question de savoir si leur intégration au sein du service des médecins-conseils contribuerait à éclaircir les choses demeure.

Relevons également la collaboration entre l'Office fédéral de la santé publique et notre service dans le cadre d'un projet ayant pour but de dégager une vue d'ensemble de la protection des données dans le domaine de la santé et de formuler des propositions de solutions. Il s'agit là d'un projet extrêmement important étant donné les transformations que connaît ce domaine, pour lequel nous ne mentionnerons que l'introduction des DRG (groupes de diagnostic). Nous escomptons les résultats de ce projet dans le courant de cette année. Autre point positif, la CSS s'est déclarée prête à se soumettre à un audit externe régulier en matière de protection des données. C'est exactement ce que nous demandons depuis longtemps pour l'ensemble du secteur de la santé afin de renforcer durablement la confiance concernant le traitement de données extrêmement sensibles.

Dans ce secteur, la nouvelle loi sur la protection des données contient un nouvel instrument très important: la certification en matière de protection des données. Nous œuvrons pour que ces procédures se généralisent en particulier lorsque des données

sensibles sont traitées. Comme le prévoit l'ordonnance sur la certification, nous sommes actuellement en train d'élaborer avec les milieux concernés les directives en la matière. L'objectif est d'établir une procédure qui soit la plus simple et la plus conviviale possible, basée sur la norme ISO 27001.

De manière générale, les influences positives de la nouvelle loi sur la protection des données, entrée en vigueur le 1er janvier 2008, apparaissent. Nous constatons en particulier que les grandes entreprises, dont les responsables de la protection des données sont membres de l'Association des conseillers d'entreprises en matière de protection des données (Verein Unternehmens-Datenschutz VUD), ont activement participé à la mise en œuvre des nouvelles dispositions. À cette occasion, elles ont recherché une collaboration constructive avec le PFPDT.

Dans le cadre de l'élaboration de la nouvelle loi sur les systèmes d'information de police de la Confédération, nous sommes parvenus, suite à un jugement rendu par la Cour européenne des droits de l'homme, à améliorer de manière significative la situation juridique des personnes désirant consulter les banques de données Janus et Gewa. Nous devons maintenant parvenir au même résultat à propos de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). En raison des risques pour la sphère privée liés à l'orientation de cette loi, dont le projet de révision est actuellement débattu au parlement, la LMSI aura une place importante dans le cadre de notre activité de cette année.

Une bonne nouvelle à propos de SWIFT: cette organisation a décidé de séparer techniquement et organisationnellement les traitements des transactions financières qui ne sont pas en lien direct avec les États-Unis. Ainsi ces transactions ne seront plus soumises de manière générale au droit américain, de sorte que l'accès aux données des transactions par les autorités américaines ne pourra plus avoir lieu dans ce cadre là. Dans cette optique, nous nous félicitons que SWIFT ait décidé d'ouvrir un centre opérationnel en Suisse. Ce centre assurera le traitement des transactions financières qui ne concernent pas les États-Unis.

La loi sur la transparence est entrée en vigueur il y a bientôt deux ans et il est maintenant possible d'établir un premier bilan. Il semble que le passage du principe du secret vers celui de la transparence se fait progressivement dans les offices fédéraux. En notre qualité d'organe de médiation, nous sommes parvenus à une solution plus favorable pour les personnes désirant consulter des documents officiels dans la plupart des cas où l'accès à ces documents avait été refusé en partie ou totalement par un organe fédéral. Toutefois, il est également apparu dans cette première phase de l'adaptation au principe de la publicité, que les offices auront encore besoin d'un certain temps pour se familiariser avec cette nouvelle situation. Un point positif est

à mentionner: dans le passé nous avons à plusieurs reprises abordé la question des ressources; la Chancellerie fédérale nous a accordé deux postes, pour une période toutefois limitée, afin de pouvoir donner suite aux nombreuses demandes de médiation reçues la première année suivant l'entrée en vigueur de la loi sur la transparence. Nous avons bon espoir que ces demandes pourront être traités d'ici la fin de l'année. Se posera ensuite la question de savoir quelles ressources doivent être définitivement mises à disposition afin d'assurer un bon fonctionnement.

Concernant l'adhésion de la Suisse aux Accords de Schengen/Dublin et leur mise en œuvre, la Suisse a dû se soumettre à une évaluation relative à son système de protection des données. Dans ce contexte nous avons accueilli durant plusieurs jours en mars une délégation européenne composée de treize experts et dirigée par le commissaire slovène à la protection des données. Les experts ont examiné l'état de la protection des données aux niveaux fédéral et cantonal. Ils ont ensuite établi leur rapport contenant un certain nombre de recommandations. Ils ont notamment relevé que l'indépendance administrative et financière des autorités en matière de protection des données n'était pas suffisamment garantie et que trop peu de ressources étaient disponibles, en particulier pour mener à bien les nouvelles tâches. Dans les six mois prochains la Suisse devra indiquer de quelle manière elle entend donner suite aux recommandations. Le PFPDT s'est attaché au cours des dernières années à attirer l'attention sur ce problème, notamment dans la perspective des futures conventions internationales, et s'emploiera à trouver en collaboration avec les services concernés une solution praticable pour que la Suisse puisse répondre aux exigences de l'Union européenne. Une autre recommandation a pour objet la collaboration entre le PFPDT et les autorités cantonales en charge de la protection des données concernant les tâches de surveillance de la Confédération et des cantons, qui se recoupent partiellement.

La première journée suisse du droit de la protection des données a été organisée le 11 janvier 2008 avec l'Université de Fribourg; cette rencontre a prouvé que la protection des données suscite un grand intérêt. Elle a en effet attiré de nombreux participants et était consacrée essentiellement à la nouvelle loi sur la protection des données, entrée en vigueur quelques jours plus tôt. La jurisprudence de l'ancienne Commission fédérale de la protection des données y a également été abordée, ainsi que la problématique du principe de la transparence en rapport avec la protection des données dans la perspective de la loi sur la transparence entrée en vigueur en 2006. Dans ce contexte, mentionnons également la Journée européenne de la protection des données organisée pour la deuxième fois le 28 janvier 2008, en collaboration avec l'Institut européen de l'Université de Zurich. À l'occasion de cette 2ème Journée européenne de la protection des données, nous avons également collaboré avec les radios DRS et RSR. Les

deux stations ont abordé durant toute la journée divers aspects de la protection des données dans le cadre de nombreuses émissions d'une haute qualité journalistique. Une équipe d'experts mise sur pied par nos soins a répondu aux nombreuses questions des auditrices et des auditeurs tout au long de cette journée.

Dans tous les cas mentionnés, une étroite collaboration avec les acteurs concernés en dehors du cercle étroit de la protection des données s'est révélée payante et a donné des résultats remarquables au regard de la protection de la sphère privée. En effet, pour parvenir à des résultats positifs, une protection des données pragmatique doit se fonder sur la coopération la plus large possible avec les potentiels intéressés.

Hanspeter Thür

Répertoire des abréviations

AAS	Accord d'Association à Schengen
ACC	Autorité de contrôle commune
ADAMS	Anti-Doping Administration and Management System
AMA	Agence mondiale antidopage
CEDP	Contrôleur Européen à la Protection des Données
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
DFJP	Département fédéral de justice et police
EAN	European Article Number
fedpol	Office fédéral de la police
FF	Feuille fédérale
IWGDPT	International Working Group on Data Protection in Telecommunications
LAA	Loi fédérale sur l'assurance-accidents
LAGH	Loi fédérale sur l'analyse génétique humaine
LAI	Loi fédérale sur l'assurance-invalidité
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LCA	Loi fédérale sur le contrat d'assurance
LDIP	Loi fédérale sur le droit international privé
LHR	Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes
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

LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi fédérale sur la protection des données
LPers	Loi sur le personnel de la Confédération
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
LRH	Loi fédérale relative à la recherche sur l'être humain
LSF	Loi sur la statistique fédérale
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
OACI	Organisation de l'aviation civile internationale
OCPD	Ordonnance sur les certifications en matière de protection des données
OFAC	Office fédéral de l'aviation civile
OFAS	Office fédéral des assurances sociales
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
OMSI	Ordonnance sur les mesures visant au maintien de la sûreté intérieure
PA	Loi fédérale sur la procédure administrative
PFPDT	Préposé fédéral à la protection des données et à la transparence
PNR	Passenger Name Record
RAI	Règlement sur l'assurance-invalidité
REE	Registre des établissements et des entreprises
RO	Recueil officiel

SAS	Service d'accréditation suisse
sedex	secure data exchange
SGPD	Système de gestion de protection des données
SGSI	Système de gestion de sécurité de l'information
SIS	Système d'information de Schengen
TAF	Tribunal administratif fédéral
UID	Numéro d'identification des entreprises

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Ordonnance sur les certifications en matière de protection des données

Dans le cadre de l'audition et de la deuxième consultation des offices, nous avons pris position sur l'ordonnance sur les certifications en matière de protection des données. Nous nous sommes clairement prononcés en faveur d'un label officiel pour la protection des données. Malheureusement, notre avis n'a pas été pris en compte. Par contre, l'ordonnance prévoit explicitement que nous devons émettre des directives concernant les exigences minimales pour un système de gestion de la protection des données.

Nous avons pris position sur le projet d'ordonnance sur les certifications en matière de protection des données (OCPD) aussi bien dans le cadre de l'audition que de la deuxième consultation des offices (interne à l'administration fédérale). A cette occasion, nous avons constaté avec regret que les projets d'ordonnance actuels ne mentionnaient plus de label pour la protection des données. Nous sommes cependant d'avis qu'un tel label est absolument nécessaire pour des raisons de transparence. Ceci permettrait aux consommateurs de se rendre compte immédiatement s'ils ont affaire à une certification selon la LPD émise par une entreprise accréditée ou non. L'entreprise certifiée pourrait de son côté utiliser le label officiel sans encourir de frais supplémentaires. Nous avons également retenu que le groupe de travail (cf. notre 14ème rapport d'activités 2006/2007, ch. 1.1.1) n'avait jamais remis en question un label de qualité officiel pour la protection des données. De plus, un tel label pourrait sans autre exister parallèlement à d'éventuels labels de qualité privés. Nous avions également insisté sur le fait qu'il fallait bien distinguer entre protection des données et sécurité de l'information, ce qui signifie qu'une simple référence aux normes internationales relatives aux systèmes de gestion,en particulier aux systèmes de gestion de sécurité de l'information (SGSI), ne suffirait pas. C'est pour cette raison que nous avions demandé que l'OCPD nous donne la compétence d'émettre des directives concernant les exigences spéciales de protection des données devant être respectées dans le cadre d'une certification, de manière analogue à ce que le projet d'ordonnance prévoyait déjà pour la certification en matière de protection des données de produits. Finalement, nous nous sommes prononcés pour que la compétence de reconnaître

des organes de certification étrangers ne soit pas octroyée à notre office, mais à l'organisme suisse d'accréditation ou à l'Office fédéral de la justice. Nous avions justifié ceci par le fait que la LPD ne nous attribue pas de compétence de décision.

Nos remarques concernant le label officiel de qualité et concernant la reconnaissance d'organismes de certification étrangers n'ont pas été prises en compte. Par contre, la version définitive de l'OCPD prévoit explicitement que c'est au PFPDT d'émettre des directives concernant les exigences minimales devant être remplies par un système de gestion de la protection des données (cf. ch. 1.1.2 du présent rapport d'activités).

La loi révisée sur la protection des données ainsi que l'OCPD sont entrées en vigueur le 1er janvier 2008.

1.1.2 Émission des directives du PFPDT pour la certification d'organisations

Selon l'Ordonnance sur les certifications en matière de protection des données (OCPD), le préposé est chargé d'édicter des directives sur les exigences minimales qu'un système de gestion de protection des données doit remplir. Pour cela, il tient compte des normes internationales relatives aux systèmes de gestion, en particulier d'ISO/CEI 27001:2005. Ces directives incorporent l'essentiel de la norme 27001 en se focalisant clairement sur la protection des données, tout en s'appuyant sur un guide d'implémentation annexe. Cette brochure structurée selon neuf principes généraux de la LPD et comprenant actuellement une vingtaine de mesures concrètes, est le pendant pour la protection des données de la norme 27002 (code de pratique pour la sécurité de l'information), associée à la norme 27001.

Suite à l'introduction du nouvel article 11 LPD concernant la procédure de certification, l'ordonnance sur les certifications en matière de protection des données (OCPD) est entrée en vigueur au 1er janvier 2008. Selon l'art. 4 al. 3 OCPD (Certification de l'organisation et de la procédure), «le préposé émet des directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir. Il tient compte des normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestion, dont en particulier les normes ISO 9001:2000 et ISO 27001:2005.»

Pour ce faire, une première étape consiste à reprendre d'ISO 27001 les exigences génériques pour les systèmes de gestion, elles-mêmes issues de celles fondamentales d'ISO 9001 pour la gestion de la qualité, comme en témoigne l'annexe informative

C d'ISO 27001. La difficulté majeure a consisté à mettre l'accent sur la protection des données, plutôt que sur la seule sécurité de l'information. Par le biais de l'art. 7 qui couvre les exigences de sécurité des données imposées par la LPD, on peut fort heureusement considérer la protection des données comme un objectif global remplaçant par extension celui de la sécurité de l'information visé par ISO 27001. On vise ainsi l'établissement d'un système de gestion de la protection des données (SGPD), qui prescrit entre autres une politique du système de gestion de la protection des données, une sélection de mesures pour le traitement des non-conformités, une déclaration d'applicabilité des mesures implémentées avec justification de celles qui auraient été exclues, un plan de traitement des non-conformités, une revue des violations ou incidents de protection des données et des actions correctives ou préventives pour améliorer le SGPD.

Dans un second temps, il s'est agi de reprendre l'annexe normative A d'ISO 27001 qui est en fait constituée de la table des matières de la norme ISO/CEI 27002:2005 plus connue sous le nom de «Code de pratique pour la gestion de la sécurité d'information». Celui-ci comprend 15 chapitres, dont les 11 derniers forment des «groupes de contrôle», eux-mêmes subdivisés en 39 «objectifs» conduisant à un total de 133 «mesures de contrôle». L'accent sur la protection des données est ici évident, étant donné la mesure 15.1.4 qui porte sur la «Protection des données et confidentialité des informations relatives à la vie privée» et qui prescrit en substance que «celles-ci doivent être garanties telles que l'exigent la législation, les règlementations applicables, et les clauses contractuelles le cas échéant».

Dans l'optique d'une certification d'organisation ou de procédure de protection des données, cette seule mesure très générale doit à l'évidence être détaillée et subdivisée en objectifs, eux-mêmes réalisables par des mesures concrètes de protection. Ceci est actuellement prévu dans le cadre d'un «Guide d'implémentation» ou encore «Code de pratique pour la gestion de la protection des données», annexé aux «Directives sur les exigences minimales qu'un SGPD doit remplir». À l'instar de l'OCDE et d'autres pays tels l'Australie, le Canada et la Grande-Bretagne, nous avons retenu «9 principes généraux de la loi sur la protection des données» comme objectifs essentiels de ce «Guide d'implémentation des directives pour SGPD». Ces objectifs se traduisent à l'heure actuelle par 20 mesures concrètes de protection des données, reprenant de manière non exhaustive les principales exigences issues de la loi ou de son ordonnance d'application. Afin de faciliter la lecture et la compréhension de cette annexe, chaque mesure est structurée conformément au standard ISO 27002, dont elle constitue une extension spécifique pour la protection des données. De même que la mesure 15.1.4 renvoie les SGSI aux SGPD, le 7ème objectif «Sécurité des données» avec ses

mesures associées n'est rien d'autre que le renvoi des SGPD aux SGSI. Parmi les 133 mesures de sécurité proposées par ISO 27002, une présélection des plus pertinentes pour la protection des données a été effectuée.

S'il n'est bien sûr pas question d'imposer une certification SGSI pour obtenir une certification SGPD, le niveau de reconnaissance d'une certification SGSI préexistante, notamment par rapport aux exigences de «Sécurité des données», devra être évalué et décidé de cas en cas par le certificateur. S'agissant de l'accréditation effectuée par le Service d'accréditation suisse (SAS), il est par contre probable que l'accréditation SGPD soit prévue comme une extension de l'accréditation SGSI (ISO 27001), étant donné la référence étroite et explicite aux exigences de cette norme.

Pour tous les acteurs concernés (accréditeurs, certificateurs, certifiés, auditeurs, contrôleurs, etc.), il faut souligner que l'actuel lien étroit avec les normes internationales ISO 27001 et 27002, sans oublier les futures normes 27003, 27004, 27005, 27006 et 27007, est judicieux et avantageux, étant donné leur importante reconnaissance et pénétration sur le marché mondial, ainsi que leur précieux apport terminologique, structurel et systématique.

Dans le but d'obtenir l'avis des milieux concernés, nous avons ouvert à fin 2007 une consultation des offices fédéraux et une audition externe. D'une manière générale, les directives proposées, ainsi que l'annexe d'implémentation, ont été plutôt bien accueillies. À la lumière des prises de position reçues, nous travaillons actuellement à une refonte rédactionnelle des directives, de manière à en améliorer la transparence et la lisibilité, en leur intégrant les éléments essentiels de la norme ISO 27001, tout en respectant les contraintes liées aux droits d'auteur. Le préposé devrait ainsi être à même d'édicter ces directives dans le courant du printemps 2008.

1.1.3 Introduction de données biométriques dans les documents d'identité

L'utilisation restreinte et réglementée de données biométriques pour permettre une meilleure authentification des personnes dans le cadre des contrôles d'identité et pour renforcer la sécurité des documents d'identité n'est pas contraire aux principes de protection des données. Par contre, l'utilisation de ces mêmes données à des fins d'identification est plus problématique et soulève de notre part des réserves.

Lors de la procédure de consultation des offices relative à l'arrêté fédéral portant approbation et mise en œuvre de l'échange de notes entre la Suisse et l'Union européenne concernant le Règlement (CE) 2252/2004 établissant des normes pour les

éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, nous avons formulé plusieurs remarques en ce qui concerne l'utilisation de données biométriques. Nous avons également fait part de notre position à la Commission des institutions politiques du Conseil des Etats et à celle du Conseil national. Le parlement n'a cependant pas suivi nos remarques et a adopté le projet présenté par le Conseil fédéral.

Le Règlement (CE) 2252/2004 qui doit être repris dans le cadre du développement de l'acquis de Schengen, de même que les recommandations de l'Organisation de l'aviation civile internationale (OACI) et les normes légales des Etats-Unis prévoient l'introduction dans les passeports et documents de voyage de données biométriques (image du visage et empreintes digitales) à des fins d'authentification (comparaison 1:1). Par authentification, on entend l'action de vérifier à l'aide d'un appareil de lecture que les données biométriques produites par la personne présentant un document d'identité correspondent aux données de référence figurant sur le support électronique contenu dans ce même document. L'opération d'authentification ne nécessite pas une centralisation des données puisque la vérification peut être effectuée directement par l'appareil au poste de contrôle. La conservation, au-delà du temps nécessaire à l'établissement des documents, des données biométriques dans le système d'information relatif aux documents d'identité (fichier ISA) et dans le système d'information relatif aux documents de voyage suisses et aux autorisations de retour pour étrangers (fichier ISR) violerait dans ce cas les principes de finalité et de proportionnalité. Cependant, nous ne sommes pas opposés aux possibilités offertes par les nouvelles technologies comme la biométrie pour permettre une meilleure authentification des personnes dans le cadre des contrôles d'identité ainsi que pour renforcer la sécurité des documents d'identité.

Par contre, nous sommes très réservés quant à l'utilisation de données biométriques à des fins d'identification (comparaison 1:n) qui implique obligatoirement une centralisation des données. Un tel traitement de données sensibles est admissible si les finalités et les droits d'accès à ces données sont suffisamment détaillés au niveau d'une base légale au sens formel (loi sur les documents d'identité). En effet, seul un cadre légal rigide peut limiter les risques d'abus et de dérapages ainsi que le risque d'utilisation des données biométriques comme clés d'accès à diverses banques de données, et partant, d'interconnexion de différents fichiers. A notre avis, la modification de la loi sur les documents d'identité proposée dans le cadre de l'arrêté fédéral susmentionné ne remplit pas les conditions susmentionnées. Pour cette raison, nous n'avons pas soutenu la conservation à des fins d'identification des données biométriques dans les fichiers ISA et ISR.

Au niveau de l'Union européenne, le groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel établi par l'article 29 de la directive 95/46/CE a, dans un avis daté du 30 septembre 2005, émis des réserves à l'égard d'une base de données nationale ou européenne sur les éléments biométriques. Le Parlement européen a même demandé l'interdiction d'une base de données centralisée des passeports et documents de voyage contenant les données biométriques et autres données personnelles de tous les titulaires d'un passeport au sein de l'Union européenne.

1.1.4 Ordonnance d'application de la loi sur l'harmonisation de registres

Nous avons été invités à prendre position sur l'ordonnance d'application de la loi sur l'harmonisation de registre dans le cadre de deux procédures de consultation. Des divergences demeurent, notamment en ce qui concerne les mesures de sécurité pour les échanges de données au niveau cantonal et communal ainsi que les modalités de contrôle de qualité des données. En outre, certains flux de données ne sont pas mentionnés.

La nouvelle loi sur l'harmonisation de registres (LHR), entrée en vigueur le 1er novembre 2006, est l'une des bases légales pour le recensement 2010. L'ordonnance d'application relative à cette nouvelle loi a fait l'objet de deux procédures de consultation de la part de l'Office fédéral de la statistique (OFS).

A l'issue des procédures de consultation dans le cadre desquelles nous avons été invités à prendre position, les divergences suivantes demeurent:

- Mesures de sécurité pour les échanges de données au niveau cantonal et communal: alors que la plateforme de communication sedex (cf. ch. 1.1.7) garantit un très haut niveau de sécurité pour les échanges des données à niveau de la Confédération les mêmes garanties ne sont pas prévues au niveau cantonal et communal. En effet, les cantons et les communes n'ont pas l'obligation de garantir le même niveau de sécurité que celui prévu dans la plateforme sedex.

- Modalités de contrôle de qualité des données: le projet d'ordonnance de l'OFS prévoit la possibilité de vérifier la qualité des données reçues, mais ne définit pas clairement les détails. Nous sommes d'avis qu'il convient de préciser que le contrôle de qualité peut être effectué uniquement sur la base de données récoltées à des fins statistiques pour le recensement fédéral de la population.

En outre, l'existence d'un service de validation de la qualité des données pose la question de savoir quels seront les flux de données dans le cas où une inexactitude des données est constatée. Or, aucune réponse à cette question n'a pour l'instant été apportée dans le projet de l'OFS.

1.1.5 Recensement 2010

Dans le cadre des travaux préparatoires en vue du recensement fédéral de la population en 2010, nous avons examiné les aspects de protection des données à prendre en compte dans le domaine de la statistique, de l'harmonisation des registres et du recensement. Nous avons collaboré avec l'Office fédéral de la statistique et pris position sur les projets de loi sur le recensement fédéral et de l'ordonnance sur l'harmonisation des registres.

En 2010, le recensement fédéral de la population sera mené selon une nouvelle méthode; pour la première fois en Suisse, le recensement sera ainsi réalisé sur la base d'informations provenant des registres administratifs et d'enquêtes par sondage auprès d'échantillons de ménages.

Dans le cadre des travaux préparatoires relatifs au recensement 2010, nous avons eu de nombreux contacts avec l'Office fédéral de la statistique (OFS), sous forme d'avis écrits ou de séances, afin de contribuer aux réflexions faites par cet office en matière de protection des données personnelles.

Lors des différentes procédures de consultation, nous avons en particulier souligné l'importance du respect du principe de finalité, du niveau de sécurité (mesures techniques et organisationnelles) pour les échanges de données dans le cadre de la loi sur l'harmonisation des registres et la loi sur le recensement, ainsi que les modalités de contrôle de qualité des données et le flux de données vers les cantons et les communes en cas d'inexactitude des données.

Dans le contexte du recensement 2010, les thématiques principales en matière de protection des données seront: l'anonymisation et l'effacement des données personnelles, le respect du principe de finalité (distinction entre buts statistiques et administratifs), la sécurité des données, le droit d'accès, les flux de données personnelles avec des tiers chargés d'effectuer des enquêtes ou le retour des données dans les cantons et communes, l'harmonisation des registres et l'utilisation du numéro AVS comme identifiant.

1.1.6 Numéro d'identification des entreprises

L'Office fédéral de la statistique prévoit d'introduire un numéro d'identification pour les entreprises. Les finalités de ce projet sont à la fois statistiques et administratives. Nous comprenons bien les avantages d'un tel système; toutefois la base légale prévue n'est pas satisfaisante. En outre, certaines applications prévues augmentent fortement les possibilités de surveillance et d'atteintes à la personnalité, en particulier les applications Business to Business.

Dans le cadre d'une consultation des offices, l'Office fédéral de la statistique (OFS) nous a soumis son projet pour un numéro d'identification des entreprises (UID). Le projet, qui devrait être mis en oeuvre en 2010 vise à faciliter les échanges d'informations à l'intérieur de l'administration (Governement to Governement, G2G), les échanges d'informations entre les entreprises et l'administration (Business to Governement, B2G) ainsi qu'entre les différentes entreprises (Business to Business, B2B). Au-delà des finalités statistiques, le projet a, aussi des finalités administratives.

Dans le cadre de son projet, l'OFS envisage de se baser sur le Registre des établissements et des entreprises (REE). L'ancrage légal de l'ordonnance relative au REE figure dans la loi sur la statistique fédérale (LSF).

Or, les finalités et les utilisations envisagées par le projet dépassent largement le cadre de la statistique. Par conséquent, une loi au sens formel doit être élaborée. Pour que l'existence d'une telle base légale soit assurée lors de la mise en service du système prévue en 2010, les travaux législatifs devraient être entrepris sans délai, en même temps que les travaux de conceptualisation technique du projet.

L'application proposée comporte des risques d'atteintes à la personnalité. En effet, les différentes activités des personnes concernées pourront être corrélées sur la base de l'UID et utilisées à des fins de profilage.

En ce qui concerne les utilisations de l'UID à l'intérieur de l'administration ainsi qu'entre les entreprises et l'administration, les explications fournies démontrent que les applications G2G et B2G répondent au principe de proportionnalité. En revanche, l'utilisation complémentaire de l'UID entre différentes entreprises augmente fortement les possibilités de surveillance et d'atteintes à la personnalité. Ces risques sont comparables à ceux pris en compte lors de la dernière révision de la Loi fédérale sur l'assurance-vieillesse et survivants (l'art. 50e LAVS limite l'utilisation du nouveau numéro AVS). Or les risques relatifs aux applications possibles dans le domaine B2B, tels que le profilage, ne sont ni analysés ni même relevés dans la documentation présentée. Nous sommes d'avis que l'utilisation de l'UID pour les applications B2B devrait être interdite, ou à tout le moins limitée, dans le cadre des dispositions à élaborer.

1.1.7 Plateforme de communication sedex

Pour permettre les transmissions électroniques des données dans le cadre de l'harmonisation des registres et du recensement 2010, l'office fédéral de la statistique a mis sur pied une plateforme de communication. Dans la conception du système, l'accent a été mis sur la protection et la sécurité des données. Le produit final répond parfaitement aux exigences de la protection des données.

L'harmonisation des registres et le recensement 2010 impliquent la transmission électronique d'une multitude de données personnelles entre les différents acteurs (autorités fédérales, cantonales et communales). Les données en question touchent tous les aspects de la vie des citoyens et ont dans ce contexte une sensibilité accrue. La nécessité d'empêcher tout accès abusif aux données est évidente. C'est dans ce cadre que l'office fédéral de la statistique (OFS) a développé la plateforme d'échange de données sedex (secure data exchange).

Sedex se base sur une infrastructure à clés publiques (Public Key Infrastructure - PKI) et sur un chiffrement robuste des informations échangées qui permet de garantir la confidentialité des données. En pratique, chaque acteur aura sa propre clé asymétrique (soit une partie publique, connue de tous les acteurs concernés, et une partie privée).

Non seulement il convient d'assurer la confidentialité des données, mais encore de vérifier que l'expéditeur des données est vraiment celui qu'il prétend être. Grâce à l'infrastructure PKI prévue dans le cadre de sedex, l'expéditeur pourra, à l'aide de la partie privée de sa clé, signer numériquement ses messages, tandis qu'à l'aide de la partie publique de la clé les destinataires pourront vérifier l'identité de l'expéditeur.

Finalement, il convient d'assurer que les messages arrivent vraiment à destination et que l'expéditeur soit le cas échéant informé de la non-livraison du message. A cette fin, la plateforme sedex garde tous les messages non encore livrés dans un serveur central. Dans la pratique, un message envoyé ne sera pas immédiatement livré au destinataire, mais déposé dans une boîte aux lettres individuelle (qui ne peut être ouverte que par le destinataire) sur un serveur central. Avec des invitations périodiques à émettre, le destinataire pourra vérifier l'éventuelle présence de messages le concernant. S'il n'est pas lu par le destinataire après un certain délai, le message sera effacé du serveur et l'expéditeur sera informé du problème afin de pouvoir réagir en conséquence. Un tel procédé permet d'avoir un contrôle sur la livraison des messages.

Vu les caractéristiques du système sedex, notre appréciation est largement positive. Ce constat a été confirmé lors de la présentation publique d'un prototype fonctionnel du système.

1.1.8 Les listes noires au regard de la protection des données

Les hôteliers et les restaurateurs sont régulièrement confrontés à des clients qui se comportent de manière inadmissible, ne payent pas leurs factures, causent des dégâts ou encore se montrent agressifs envers d'autres clients. Des aubergistes, gérants de club ou hôteliers lésés se sont adressés à nous en nous demandant s'ils pouvaient créer une banque de données commune à des établissements analogues afin de s'épargner des surprises désagréables. Nous avons conclu qu'il pouvait exister un intérêt privé prépondérant pour établir un tel fichier et avons précisé à quelles conditions une telle mesure était admissible.

Des responsables d'établissements d'hôtellerie-restauration et d'établissements apparentés confrontés à des comportements inadmissibles de la part de certains clients malveillants nous ont demandé s'ils pouvaient établir une banque de données afin d'empêcher ces personnes de nuire et de protéger autant que possible leurs établissements.

La collecte d'informations sur des personnes au comportement inadmissible et leur enregistrement dans une banque de données constitue un traitement de données au sens de la LPD. Celui-ci pouvant porter atteinte à la personnalité des personnes concernées, la personne qui collecte ces données doit disposer d'un motif justificatif pour procéder au dit traitement. En l'occurrence, l'intérêt prépondérant privé des exploitants peut en principe justifier un traitement de données personnelles. La personne qui procède au traitement des données doit toutefois respecter les principes généraux de la LPD. Elle doit notamment informer clairement les personnes concernées du but et des conditions du traitement des données (principe de transparence) et ne peut traiter que les données personnelles propres et nécessaires au but poursuivi par le traitement des données (principe de finalité et de proportionnalité).

Nous avons dans ce contexte défini un certain nombre de règles afin que la mesure envisagée respecte la LPD et ses principes et nous avons recommandé aux gérants d'établissements d'établir un concept pour le traitement de données avant la mise en œuvre d'une telle mesure. Ces règles se trouvent dans l'annexe 4.1.

1.1.9 Protection de la personnalité post mortem

La protection des données est une protection de la personnalité. Les controverses juridiques concernant la personnalité et l'atteinte à la personnalité sont donc pour nous d'une importance majeure. Une controverse qui refait surface régulièrement dans ce contexte concerne la protection de la personnalité après la mort. A nos yeux, elle est importante surtout en rapport avec le droit d'accès: le cas de l'accès aux données après le décès de la personne concernée est certes réglé dans l'ordonnance sur la protection des données, mais dans la pratique, l'application de la disposition est jalonnée de questions en suspens.

Le plus simple est d'illustrer cette question complexe du point de vue juridique à l'aide d'un exemple concret. Ainsi, la question de la protection de la personnalité post mortem se pose par exemple lorsqu'une personne demande à consulter les dossiers d'une compagnie d'assurance concernant un proche décédé et que l'assureur refuse de les lui remettre en invoquant la protection des données.

En principe, du point de vue de la protection des données, la retenue de l'assureur est adéquate. Mais dans le cas présent, on ne peut s'arrêter là, car l'ordonnance relative à la loi fédérale sur la protection des données (OLPD) accorde aux proches un droit de consulter les données lorsqu'ils justifient d'un intérêt à la consultation et qu'aucun intérêt prépondérant de tiers ne s'y oppose. Toutes les personnes qui peuvent invoquer un lien de proche parenté ou de mariage avec la personne décédée n'ont pas besoin d'apporter la preuve d'un intérêt (art. 1, al. 7, OLPD).

Même à ce stade de l'examen du cas, il ne faut pas prendre les choses trop à la légère: le fait qu'un intérêt soit établi en cas de proche parenté ou de mariage avec la personne décédée ne dispense toutefois pas d'une pondération des intérêts en présence. Il faut s'enquérir des motivations des parties, tant pour l'exigence que pour le refus de la communication des données.

La jurisprudence concernant la communication de données aux proches est plutôt restrictive. Si les données sont requises dans le cadre d'un litige juridique, il faut restreindre leur communication aux informations se rapportant à l'objet futur du procès. S'il s'agit de dossiers médicaux, il convient en outre d'examiner si et dans quelle mesure la protection de la personnalité de la personne décédée peut être garantie en n'autorisant pas une consultation directe des dossiers, mais en communiquant les informations par l'intermédiaire d'un médecin qui lui, aura eu accès au dossier (fonction de filtre).

La pondération des intérêts ne peut être effectuée que sur la base des données se rapportant au cas concret. Nous ne pouvons donc pas apprécier de manière définitive les demandes de consultation de données. Dans l'exemple cité plus haut, nous avons néanmoins établi un inventaire des principaux arguments afin de promouvoir dans la mesure du possible une solution consensuelle entre les parties.

1.2 Protection des données – Questions d'ordre géneral

1.2.1 Engagement d'appareils de surveillance à la frontière suisse

L'ordonnance régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Administration fédérale des douanes, entrée en vigueur le 1er mai 2007, crée des dispositions d'exécution détaillées pour l'utilisation d'appareils de surveillance à la frontière suisse. Elle indique les appareils autorisés ainsi que leurs domaines d'utilisation et règle les responsabilités ainsi que la durée de conservation des relevés.

Pour la troisième fois de suite, nous avons abordé le sujet de l'engagement d'appareils de surveillance (tels que les drones de reconnaissance et les hélicoptères équipés de systèmes à infrarouges) à la frontière suisse (cf. 13ème rapport d'activités 2005/2006; ch. 2.2.1, 14ème rapport d'activités 2006/2007, ch. 1.2.2). Le projet d'«Ordonnance régissant l'utilisation d'appareils de prises de vue, de relevé et d'autres appareils de surveillance par l'Administration fédérale des douanes», que l'administration des douanes a soumis à la consultation des offices, nécessitait de nombreuses améliorations du point de vue de la protection des données.

Ainsi, nous nous sommes opposés à la formulation bien trop générale selon laquelle les appareils autorisés pouvaient «capter et enregistrer des signaux visuels fixes ou mobiles» et des «signaux acoustiques». Nous avons demandé, pour des raisons de transparence et conformément au principe de proportionnalité, d'énumérer de manière exhaustive tous les appareils devant effectuer ce genre de surveillance (tels qu'appareils photographiques, caméras à infrarouge, détecteurs de mouvement, radiogoniomètres). Nous avons également demandé que l'ordonnance décrive clairement le domaine d'utilisation de chaque appareil de surveillance et qu'elle fixe de manière exhaustive les finalités pour lesquelles ceux-ci peuvent être utilisés. Nous nous sommes également opposés à une durée de conservation de trois mois et nous sommes finalement mis d'accord avec l'administration des douanes sur le fait que les relevés devaient en principe être détruits au bout d'un mois.

Nous avons également proposé d'inclure une disposition qui fixe deux principes importants pour chaque engagement: premièrement, chaque engagement mobile doit être limité dans le temps. Deuxièmement, le public doit être informé par des mesures appropriées de l'utilisation des appareils de surveillance (par exemple par des panneaux indicateurs ou par une information préalable sur Internet ou dans les médias

locaux), conformément au devoir d'informer prévu dans la loi révisée sur la protection des données. Cette indication peut être omise uniquement dans les cas où elle mettrait en péril le but de l'engagement.

L'administration des douanes a en grande partie accepté nos remarques et adapté les dispositions concernées. Par contre, nous n'avons pas réussi à obtenir que l'ordonnance décrive les secteurs dans lesquels aucune surveillance n'est permise, telles que les régions à population dense, l'intérieur du pays. Nous nous étions basés sur une prise de position du Conseil fédéral sur la motion 05.3804, dans laquelle il s'était explicitement prononcé contre une utilisation de drones dans ces deux secteurs. Le fait que notre exigence n'ait pas été prise en compte est à déplorer, surtout du fait que l'ordonnance autorise maintenant non seulement l'utilisation de drones, mais aussi de nombreux autres appareils de surveillance.

1.2.2 Surveillance à l'aide de microdrones

L'office fédéral de l'aviation civile s'est adressé à nous au sujet de l'utilisation de microdrones équipés de caméras. La règle générale est que toute personne qui désire utiliser de tels microdrones à des fins de surveillance doit respecter les exigences de la loi sur la protection des données.

L'OFAC a été confronté à plusieurs reprises à des mises en service possibles de microdrones. Un microdrone est un aéronef sans pilote qui pèse moins de 30 kilos et qui, selon la législation actuelle, ne nécessite pas d'autorisation. L'OFAC examine actuellement s'il y a lieu d'assujettir ces microdrones à une obligation d'autorisation et si oui, sous quelle forme. Les microdrones pouvant également être équipés de caméras, l'office fédéral s'est adressé à nous. La règle générale est que toute personne qui désire utiliser de tels microdrones équipés de caméras à des fins de surveillance doit respecter les exigences de la loi sur la protection des données dès lors que des personnes identifiées ou identifiables sont prises dans le champ de vision de la caméra. Nous avons communiqué à l'OFAC que nous apprécierions qu'il mentionne de son côté que la législation sur la protection des données doit être prise en compte, soit dans le cadre d'une procédure d'autorisation, soit d'une autre manière. L'OFAC va maintenant élaborer un concept préliminaire au sujet des microdrones et nous consultera pour les aspects touchant à la protection des données.

1.2.3 L'utilisation de technologies respectueuses de la protection des données dans le domaine de la surveillance par vidéo

Du point de vue de la protection des données, la vidéosurveillance ne devrait être utilisée que dans les cas où d'autres mesures qui portent moins atteinte à la personnalité des personnes concernées ne sont pas disponibles. Si une vidéosurveillance est effectuée, il convient – en particulier dans le domaine public et dans le secteur des services – d'engager autant que possible des technologies respectueuses de la vie privée.

Du point de vue de la protection des données il n'y a rien à objecter contre une vidéosurveillance effectuée au service de la sécurité aussi longtemps que son utilisation n'entrave pas les droits et les libertés liées au traitement des données personnelles. Les technologies respectueuses de la protection des données utilisées pour la vidéosurveillance doivent toujours respecter le principe de la proportionnalité. Selon ce dernier, ne peuvent être traitées que les données personnelles – dont font partie les images de personnes –nécessaires et propres à atteindre l'objectif préalablement déterminé de manière précise.

Il existe actuellement des technologies dans le domaine de la vidéosurveillance qui permettent de brouiller les objets enregistrés, en particulier les personnes, jusqu'à ce qu'ils soient méconnaissables, ce qui revient à crypter les données. En cas de nécessité, par exemple en présence d'un délit, les objets ainsi brouillés peuvent après coup être décryptés et rendus identifiables. Grâce à cette technologie, il est maintenant possible de surveiller des lieux publics sans porter atteinte à la sphère privée.

Pourtant, même une telle vidéosurveillance plus respectueuse de la protection des données ne peut garantir que des données personnelles ne soient traitées de manière abusive. Le plus important lors de l'engagement de ces technologies est que seul un cercle très restreint de personnes dignes de confiance soit autorisé à procéder au décryptage des objets brouillés. La solution la plus appropriée consiste à déléguer cette responsabilité selon le principe des quatre yeux à deux personnes au minimum. Ce n'est qu'ainsi qu'il sera possible de lutter efficacement contre les traitements de données abusifs.

1.2.4 Loi fédérale sur les systèmes militaires d'information

La dernière version du projet de loi fédérale sur les systèmes militaires d'information mis en consultation des offices en septembre 2007 contient une réglementation plus détaillée de l'utilisation de moyens de surveillance que les versions précédentes.

Dans le cadre des travaux de révision de la législation militaire (cf. notre 14ème rapport d'activités 2006/2007, ch. 1.2.3), nous avons indiqué au Département fédéral de la défense, de la protection de la population et des sports (DDPS) notre opposition à une réglementation succincte de l'utilisation de moyens de surveillance. Toute forme de surveillance étatique constitue une atteinte grave aux droits fondamentaux et doit être fondée sur une base légale claire et suffisamment détaillée. Le DDPS a mis en consultation des offices en septembre 2007 une nouvelle version du projet de loi fédérale sur les systèmes militaires d'information qui contient une réglementation plus détaillée de l'utilisation des moyens de surveillances. Ces dispositions définissent l'organe responsable de l'engagement des moyens de surveillance, mais également les buts poursuivis par ces mesures, de même que les règles relatives aux traitements des données personnelles (collecte, communication et conservation). Le projet de loi a été transmis au parlement.

1.2.5 Suivi du contrôle au centre sportif KSS et utilisation de systèmes de reconnaissance biométrique

Le suivi de la mise en place des recommandations a permis de constater l'acceptation et l'implémentation de toutes les recommandations, à l'exception de l'exigence de stockage décentralisé dont la mise en place est à ce jour encore incertaine.

Suite au contrôle effectué auprès des établissements de sports et détente «KSS Sport- und Freizeitanlagen Schaffhausen», nous avons publié en 2006 un rapport comprenant cinq recommandations concernant le système de reconnaissance biométrique utilisé par KSS pour le contrôle d'accès.

Ainsi, nous avons recommandé: la proposition d'une solution de rechange au même prix pour les personnes opposées au prélèvement de leurs données biométriques, le stockage décentralisé des données sur une puce de la carte d'abonné, l'effacement automatique des données clients dans un délai de 18 mois à compter du dernier contact, l'anonymisation des données de transaction, l'effacement des données biométriques encore stockées dans la base de données dans un délai de trois mois.

Au cours de l'année écoulée, nous nous sommes rendus à deux reprises au centre KSS afin de connaître l'état d'avancement de la mise en place des recommandations. Nous avons ainsi pu constater qu'à l'exception du stockage décentralisé, les recommandations on été acceptées et mises en œuvre.

Il ressort de la dernière séance que la mise en place de la recommandation concernant le stockage décentralisé serait possible dès janvier 2009. La KSS a confirmé en février 2008 qu'elle n'acceptait pas notre recommandation. Nous examinons la suite à donner à ce cas.

Dans ce contexte, nous avons procédé à une analyse approfondie de l'influence des systèmes de reconnaissance biométrique sur la liberté personnelle.

Les grandes lignes de nos travaux portent sur le fonctionnement des différentes technologies actuellement utilisées, la réglementation et les critères d'évaluation des facteurs relatifs à la vie privée concernant les systèmes de reconnaissance biométrique.

En outre, nous avons participé à un symposium traitant des principales questions que soulèvent l'utilisation croissante de systèmes de reconnaissance biométrique pour identifier ou authentifier les êtres humains et la création de biobanques rassemblant un nombre de plus en plus important d'échantillons biologiques.

1.2.6 La pertinence des extraits du registre des poursuites

La réputation de solvabilité revêt une importance capitale au niveau de la participation à la vie économique. Donnant des renseignements à ce sujet, l'extrait du registre des poursuites est un document extrêmement délicat. Mais certains ne comprennent parfois pas que quelques inscriptions reportées dans l'extrait n'ont rien à voir avec la solvabilité. La tentative d'une initiative parlementaire d'éliminer les dangers d'interprétation erronée a échoué devant la multitude des points de vue sur la manière dont cela devrait avoir lieu.

En premier lieu, une poursuite n'est rien d'autre que l'allégation d'une dette pécuniaire. La personne qui se défend avec succès contre cette allégation a grand intérêt à ce que l'extrait du registre des poursuites ne donne aucun renseignement à ce sujet. Il en va de même lorsque l'allégation n'est pas corroborée suite à l'opposition de la personne concernée et que la poursuite ne peut donc plus être menée au-delà d'un an. Les données figurant dans l'extrait du registre des poursuites ne donnent aucun renseignement sur la solvabilité car la poursuite ne permet pas de conclure à un manque de liquidités de la personne concernée.

Sur proposition de l'ancien conseiller national Jean Studer, une initiative parlementaire a été lancée (04.467 e Iv.pa.) grâce à laquelle le risque de malentendus aurait dû être au moins minimisé. La proposition consistait à raccourcir, dans l'extrait du registre, la durée d'annonce des poursuites dont la continuation n'a pas été requise (révision de l'art. 8a LP). La commission juridique du Conseil des Etats, chargée du traitement de cette initiative, a requis l'avis de du PFPDT ainsi que celui d'autres organismes spécialisés en matière de poursuite.

Nous avons attiré l'attention de la commission sur le fait qu'une réduction de la durée de publication ne supprimerait pas le problème car les extraits du registre des poursuites, une fois requis, continuent à circuler dans le secteur privé, notamment par le biais des renseignements en matière de solvabilité donnés par les sociétés de renseignements économiques. Celles-ci ne sont manifestement pas toutes conscientes que la communication d'anciens extraits du registre des poursuites n'est pas compatible avec la loi sur la protection des données (l'actualité des données en tant qu'aspect de l'exactitude des données).

Dans ce contexte, nous sommes d'avis qu'il ne peut y avoir de protection sûre face aux erreurs d'interprétation portant atteinte au crédit d'une personne que si les inscriptions problématiques mentionnées plus haut ne sont plus du tout mentionnés sur les extraits. Nous avons recommandé à la commission de tenir compte de ce point dans le cadre de la révision de l'art. 8a LP.

La plupart des autres participants à la consultation étaient d'avis que la pertinence des extraits du registre des poursuites laissait à désirer, mais avaient d'autres conceptions sur la manière de remédier au mieux à cette situation. Quelques voix se sont également élevées pour dire que les intérêts des débiteurs étaient déjà largement pris en compte et qu'ils n'avaient pas besoin d'une protection supplémentaire. Compte tenu des divergences parfois considérables entre les avis remis, l'initiative parlementaire Jean Studer a été finalement classée. Nous allons continuer à oeuvrer en faveur d'une protection contre les traitements de données qui portent atteinte au crédit des personnes au moyen de mesures dans le domaine privé (cf. également le chiffre 1.8.3 du présent rapport d'activités).

1.2.7 Annonce des passagers auprès des autorités douanières et policières dans le cas d'un aérodrome dépourvu de douane

Dans le cadre des vols transfrontaliers vers des aérodromes suisses ne disposant pas d'une douane, le pilote doit annoncer les passagers à l'aide d'un formulaire à remplir sur le site web de l'aérodrome. Les données sont ensuite envoyées par courriel non sécurisé aux autorités douanières et policières. En raison du nombre restreint de personnes concernées et de l'existence de nombreux aérodromes disposant d'une douane, nous sommes d'avis qu'une déclaration de protection des données constitue une mesure adéquate.

En Suisse, quelques petits aérodromes ne disposent pas d'une douane. Les avions venant de l'étranger ont le droit d'y atterrir, toutefois les formalités douanières doivent être accomplies avant le départ. Le pilote doit en particulier annoncer tous les passagers (y compris lui-même) à l'aide d'un formulaire à remplir sur le site Internet de l'aérodrome. Les données sont ensuite envoyées aux autorités douanières et policières par courriel non sécurisé. Alors qu'il était possible il y a peu d'accomplir cette formalité par téléfax, un nouveau règlement des douanes impose désormais que ces formalités soient accomplies par voie de messagerie électronique. La question qui se pose est de savoir si une transmission de ces données par courriel non sécurisé est admissible.

En tenant compte du fait que les passagers ont la possibilité de choisir un des nombreux aérodromes disposant d'une douane et que le nombre de personnes concernées est très restreint, nous sommes d'avis que la mise en place d'un système de courriels sécurisés serait disproportionnée. Nous avons par contre exigé que les aérodromes concernés publient une déclaration de protection des données sur leurs sites Internet et sur les formulaires d'annonce des douanes.

À la lumière de la loi fédérale sur la protection des données (LPD), la déclaration de protection des données devra être la plus transparente possible et contenir au moins les informations suivantes: les finalités du traitement pour lesquelles les données sont collectées, les catégories de destinataires des données, le temps de conservation des données et le fait que les transmissions des données ne sont pas sécurisées.

1.2.8 Protection des données auprès des fondateurs d'entreprises dans le domaine des médias électroniques

Les possibilités offertes par les médias électroniques génère des idées et des projets commerciaux novateurs, impliquant un traitement de données personnelles. Les fondateurs d'entreprises ne tiennent cependant pas toujours compte des exigences de la protection des données dans le cadre de leurs projets commerciaux; il peut parfois en résulter un risque accru d'atteinte à la personnalité en raison d'un usage impropre des produits ou des services électroniques offerts. Pour cette raison, nous invitons expressément les fondateurs d'entreprise, surtout en présence de projets novateurs dans le monde numérique, à faire preuve d'une plus grande attention eu égard aux problèmes de protection des données.

Les médias électroniques offrent aujourd'hui des possibilités de plus en plus variées d'élaboration de nouveaux modèles commerciaux et ont élargi l'offre de produits et de services numériques sur Internet ou sur les canaux d'information mobiles. Or, dans ce contexte, les fondateurs d'entreprises négligent souvent la protection des données. Même si dans le cas des produits et services numériques, il est parfois impossible d'offrir une protection des données absolue en raison du modèle commercial, le prestataire doit toutefois minimiser le risque d'atteinte à la personnalité qui naît d'un usage impropre de son offre. Examinons un cas concret: une entreprise offre un service permettant d'envoyer des SMS à des abonnés enregistrés sur la base du numéro de plaque du véhicule. L'enregistrement auprès de ce service peut également se faire par SMS: le message envoyé contient alors aussi le numéro du véhicule. De cette manière, un numéro de téléphone portable se voit associé à un numéro de véhicule et le supposé conducteur ou détenteur du véhicule peut donc recevoir des informations par l'intermédiaire de ce service SMS.

Du point de vue de la protection des données, ce modèle commercial renferme le risque qu'une tierce personne enregistre sur son téléphone portable le numéro de plaque d'un véhicule dont il n'est pas le détenteur ou qu'il n'utilise pas. Cela pourrait même se passer à l'insu et sans l'accord du détenteur ou du conducteur. On peut ainsi imaginer qu'un homme jaloux fasse enregistrer le véhicule de son amie sur son téléphone portable pour savoir si d'autres automobilistes d'adressent à elle. Selon son ampleur, ce procédé pourrait même être assimilé à une surveillance partielle. Afin d'éviter ce genre de situation, il faut prendre les mesures de sécurité adéquates pour l'inscription à ce service.

Par ailleurs, le service de SMS ne peut fonctionner que si son utilisation est rapide et facile. La demande serait certainement très faible si ce service nécessitait des enregistrements longs et laborieux. Il a donc fallu rechercher des solutions permettant d'empêcher ce genre d'abus et de minimiser le risque d'atteinte à la personnalité sans détruire le modèle commercial du prestataire. Nous avons recommandé à celui-ci, après l'enregistrement d'un numéro de plaque, de comparer le nom de la personne enregistrée et le nom du détenteur du véhicule (ce nom est accessible au public) et de limiter le nombre des véhicules pouvant être enregistrés sur un téléphone portable. En outre, le prestataire a la possibilité de créer un mode d'enregistrement spécifique dans lequel les données d'identité sont vérifiées.

Par ces mesures, il serait certes possible de limiter le risque d'atteintes à la personnalité, mais pas de les exclure totalement et des mesures plus poussées auraient empêché la réalisation du modèle commercial. Cela dit, le prestataire du service peut se voir confronté à une plainte civile en cas d'atteinte à la personnalité. Il prend donc encore un risque considérable en offrant son service.

1.3 Internet et télécommunication

1.3.1 Bourses d'échange sur Internet et protection des données

Nous avons examiné le traitement des données effectué par entreprise suisse active dans le domaine de la lutte contre les violations du droit d'auteur et constaté que la collecte des données effectuée dans les réseaux d'échange pair à pair ne respectait pas les principes fondamentaux de la LPD. Ce faisant, nous ne remettons nullement en cause la légitimité des poursuites pénales contre les violations des droits d'auteur. Nous avons cependant constaté qu'en pratique, les détenteurs du droit d'auteur abusent de leur droit d'accès aux dossiers dans le cadre d'une procédure pénale afin d'obtenir les identités des détenteurs d'accès Internet, contournant ainsi le secret des télécommunications dans le domaine du droit privé. Nous estimons qu'une atteinte au secret des télécommunications dans le domaine civil nécessite une base légale expresse. Nous avons recommandé à l'entreprise concernée de cesser le traitement des données.

Mandatée par l'industrie des médias, une entreprise suisse effectue des recherches dans des réseaux pair à pair (P2P) dans le but de déceler des violations du droit d'auteur commises au sein des sites d'échange de fichiers musique et vidéo sur Internet. L'entreprise en question a développé spécialement à cet effet un logiciel qui collecte secrètement et de manière automatisée les traces électroniques laissées par l'utilisateur du logiciel P2P mettant illégalement à disposition les œuvres protégées par le droit d'auteur. Ces données, comprenant notamment les adresses IP, sont enregistrées à l'insu des personnes concernées (y compris du détenteur de l'accès Internet qui peut être de bonne foi) et communiquées à intervalles réguliers aux détenteurs des droits d'auteur de l'œuvre concernée ou à leurs représentants légaux, le plus souvent à l'étranger.

Les données relatives à l'adresse IP détenues par les fournisseurs de services de télécommunications (telles que le nom et l'adresse du détenteur de l'accès Internet) sont protégées par le secret des télécommunications. Ce n'est que dans le cadre d'une enquête pénale que les autorités d'instruction peuvent obtenir l'identité du détenteur de l'accès Internet. C'est pour cette raison que les détenteurs des droits d'auteur ou leurs représentants légaux déposent une plainte pénale contre inconnu auprès des autorités d'instruction compétentes, en fournissant les données collectées par la société X. SA. Ils accèdent alors au dossier dans le cadre de la procédure pénale et se

procurent ainsi l'adresse du détenteur de l'adresse IP (qui n'est pas nécessairement la personne ayant commis l'infraction). Ils font alors valoir leurs prétentions civiles en exigeant des dommages-intérêts pour la mise à disposition de l'œuvre, avant même la condamnation pénale de l'auteur de l'infraction.

Les données collectées (en particulier l'adresse IP) sont des données personnelles dès lors qu'elles permettent d'identifier de façon indirecte des personnes déterminées. Le traitement de ces données est régi par la LPD. Les méthodes de traitement utilisées par la société X. SA pouvant porter atteinte à la sphère privée d'un grand nombre de personnes et à leur insu, nous avons procédé à un examen des faits.

Nous avons examiné si les principes de la protection des données étaient respectés, en particulier les principes de licéité, de finalité, de bonne foi et de transparence, ainsi que le principe de la proportionnalité. Nous avons également examiné s'il existait un motif - en particulier un intérêt privé prépondérant - justifiant une telle collecte de données.

Selon le principe de licéité, les données personnelles ne peuvent être traitées que de manière licite. La législation en vigueur ne permet pas expressément une collecte systématique d'adresses IP dans des bourses d'échange, ni ne l'interdit. Nous sommes toutefois d'avis qu'un tel traitement de données – effectué à l'insu des personnes concernées, de manière proactive, à des fins de procédures pénales - devrait faire l'objet d'une base légale explicite.

Selon le principe de finalité, les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. En l'occurrence, les données de connexion sont rendues accessibles afin de permettre l'échange des contenus. La collecte et l'enregistrement systématiques des données dans le but de traquer des violations du droit d'auteur ne sont pas conformes au but poursuivi à l'origine; ce changement de finalité n'est pas prévu par une loi et n'est pas non plus reconnaissable pour les utilisateurs du logiciel – et en aucun cas pour le détenteur de l'adresse IP. Ce faisant, la société X. SA ne respecte pas le principe de la finalité.

Selon le principe de transparence, un traitement de données doit être reconnaissable pour la personne concernée; la personne concernée doit en être informée ou doit s'y attendre au vu des circonstances. Dans le cas d'espèce, la collecte des données est effectuée à l'insu des personnes concernées (que ce soit le détenteur de l'accès Internet ou la personne mettant effectivement à disposition les fichiers protégés) et ceux-ci ne peuvent en principe pas s'y attendre. Dans ces conditions, la société X. SA ne respecte donc pas non plus le principe de la transparence.

Un traitement de données doit également respecter le principe de la bonne foi. En l'espèce, les données sont collectées par la société X. SA dans le but d'identifier le détenteur de l'accès Internet pour formuler ensuite à son encontre des revendications civiles. Les données relatives à l'adresse IP sont protégées par le secret des télécommunications et une identification du détenteur d'un tel accès n'est actuellement possible que dans le cadre d'une procédure pénale. En déposant une plainte pénale dans le seul but de constater l'identité du détenteur de l'accès Internet (qui, rappelons-le, peut être de bonne foi), afin lui réclamer des dommages-intérêts, les détenteurs des droits d'auteur ou leurs représentants légaux contournent le secret des télécommunications valable dans le domaine civil. Nous avons estimé qu'une telle démarche devait être considérée comme contraire au principe de la bonne foi. Dans la pratique, les titulaires des droits d'auteur utilisent le droit d'accès au dossier de la procédure pénale pour faire valoir des prétentions civiles envers le détenteur de l'adresse IP, sans même attendre la fin de la procédure pénale et la condamnation de l'auteur de l'infraction. Nous avons estimé que cette pratique constituait un abus de droit. La législation ne prévoit pas la possibilité de lever le secret des télécommunications en droit privé et cette lacune n'a pas été comblée lors de la dernière révision de la loi sur le droit d'auteur.

En ce qui concerne l'examen du principe de proportionnalité, un traitement de données peut être considéré comme proportionné s'il est nécessaire et approprié au but poursuivi et si les mesures prises sont raisonnables par rapport à l'atteinte à la personnalité de la personne concernée. En l'occurrence, le traitement effectué par la société X. SA est une mesure propre à délimiter le cercle des personnes suspectées de violer le droit d'auteur et à établir les faits d'une telle infraction afin de pouvoir ensuite déposer une plainte qui aie de bonnes chances de succès. Cette mesure est également nécessaire pour constater qu'une violation du droit d'auteur a été commise et pour pouvoir démontrer l'infraction. Les détenteurs des droits d'auteur ne doivent cependant pas forcément connaître l'identité du détenteur de l'accès Internet de bonne foi pour exercer leurs droits de partie dans le cadre d'une procédure pénale et dans ces circonstances seule la collecte de données personnelles à des fins de procédure pénale peut être estimée comme proportionnée.

Seul un intérêt prépondérant privé pourrait permettre de justifier le traitement de données effectué par la société X. SA. Le traitement des données entrepris par les titulaires des droits d'auteur (en l'espèce par la société X. SA) oppose d'une part l'intérêt des détenteurs des droits d'auteur à poursuivre en justice les personnes violant leurs droits, d'autre part les intérêts des personnes concernées au respect des droits de la personnalité.

En l'occurrence, il apparaît que dans la pratique, le droit d'accès est utilisé de façon abusive pour faire valoir des prétentions civiles contre les détenteurs d'accès Internet de bonne foi, L'abus de droit ne peut être justifié par aucun motif justificatif. Etant donné qu'il n'est pas possible de garantir que la collecte et le traitement de données effectué par la société X. SA soient limités à la poursuite pénale et aux revendications civiles des seuls auteurs de l'infraction, nous avons estimé qu'il fallait faire cesser le traitement des données.

En conclusion, nous avons constaté que le traitement de données effectué par la société X. SA ne respecte pas les principes fondamentaux de la LPD et que l'intérêt privé légitime des titulaires de droit d'auteur ne peut pas être considéré comme un motif justificatif suffisant tant qu'il n'est pas garanti que les identités des détenteurs d'accès Internet qui sont de bonne foi sont protégées dans le cadre d'une procédure pénale.

Nous avons recommandé à la société X. SA de mettre fin immédiatement au traitement de données qu'elle effectue, aussi longtemps qu'une base légale appropriée n'est pas élaborée. L'entreprise suisse a communiqué dans le délai imparti qu'elle n'acceptait pas notre recommandation. Nous avons alors porté l'affaire devant le Tribunal administratif fédéral pour décision.

1.3.2 Protection des données dans le cadre de la téléphonie sur Internet (Voice over IP)

La téléphonie sur Internet étant depuis quelques années en forte expansion, nous avons décidé d'analyser ce domaine en nous intéressant en particulier aux problèmes potentiels d'atteinte à la personnalité. Dans le but de donner des conseils utiles aux utilisateurs et aux développeurs, nous avons examiné six logiciels gratuits de téléphonie sur Internet. Un extrait du rapport se trouve à l'annexe 4.2; le rapport complet figure sur notre site web www.leprepose.ch.

1.3.3 Publication involontaire de données personnelles sur Internet

Un cas de publication involontaire sur Internet, exceptionnel de par l'ampleur et le caractère sensible des données publiées, montre une fois de plus qu'il est très important d'appliquer soigneusement les mesures organisationnelles et techniques exigées par la loi sur la protection des données.

On nous signale régulièrement des cas de données personnelles qui ont par mégarde été rendues accessibles sur Internet en raison de mesures de sécurité insuffisantes. En 2007, nous avons pris connaissance d'un cas plutôt exceptionnel aussi bien de par le nombre de personnes concernées que par le caractère sensible des données rendues accessibles. Il s'agissait d'un fichier texte de plus de 50 mégaoctets stocké sur un serveur web. Le fichier, librement accessible sur Internet, contenait des données relatives à des dizaines de milliers de personnes; outre le nom, l'adresse postale, l'adresse de courriel et la date de naissance des personnes concernées, se trouvaient également des données sur leur santé. Il s'agissait donc de données personnelles sensibles au sens de la loi sur la protection des données.

Le fichier en question était stocké sur un serveur web d'un fournisseur de prestations Internet; il y avait été mis à disposition par erreur par un client. Pendant plusieurs semaines, personne ne s'est rendu compte de cette méprise. Après avoir été informés sur cet état de fait, nous avons contacté l'entreprise concernée et demandé que ces données soient de suite retirées du réseau, ce qui a été fait immédiatement. Nous avons également demandé que des mesures soient prises pour éviter qu'un tel incident ne puisse se reproduire à l'avenir.

L'entreprise exploitante nous a assurés que l'analyse du fichier log avait révélé qu'il n'y avait heureusement eu que très peu d'accès à ce fichier par Internet.

1.4 Justice/Police/Sécurité

1.4.1 Protection des données dans le cadre de l'évaluation Schengen

La mise en œuvre de l'Accord d'Association à Schengen est évaluée par l'Union européenne avant que le Système d'Information Schengen (SIS) ne soit mis en fonction en Suisse. Lors de la visite d'évaluation auprès des autorités de protection des données suisses, ce sont les compétences du préposé fédéral et de plusieurs autorités cantonales de protection des données qui sont inspectées.

L'Accord d'Association à Schengen (AAS) - ratifié par la Suisse en mars 2006- est entré en vigueur le 1er mars 2008. Son application est subordonnée à une décision du Conseil de l'UE. Cette dernière doit être prise à l'unanimité des Etats participant à l'espace Schengen après évaluation de la capacité de la Suisse à mettre en œuvre ledit accord. Ensuite seulement, le fichier national du SIS est mis en fonction opérationnellement en Suisse. L'évaluation est menée par des équipes composées d'experts du Conseil européen, de la Commission européenne et des Etats membres. Elle porte sur la coopération policière, la protection des données, le contrôle aux frontières extérieures, les visas, la coopération consulaire et la gestion du fichier national du SIS (N-SIS).

L'évaluation de la protection des données porte sur la mise en œuvre de l'AAS, en particulier sur les compétences de l'autorité de contrôle fédérale (PFPDT) et des autorités de contrôle cantonales en matière de protection des données. Celles-ci sont évaluées sur la base d'un questionnaire et d'inspections locales. L'évaluation porte en particulier sur les compétences de surveillance, d'investigation et d'intervention des autorités de contrôle ainsi que sur leur indépendance. Ce sont les bases légales et spécialement les compétences de contrôle sur le SIS et les services impliqués dans sa gestion qui sont analysées. Les droits des personnes concernées et la sécurité des données sont également soumis à évaluation.

Nous nous sommes fortement investis dans le cadre de la préparation de cette évaluation, en étroite collaboration notamment avec l'Office fédéral de la Justice, l'Office fédéral de la Police, l'Office fédéral des migrations et les autorités cantonales de protection des données. Il s'agissait de répondre au questionnaire d'évaluation adressé à la Suisse par l'UE (février 2008) et de se préparer en vue des inspections locales (premier semestre 2008). La visite d'évaluation en matière de protection des données auprès des autorités de contrôle suisses a eu lieu au mois de mars 2008. Les

experts européens ont inspecté les compétences du PFPDT et de plusieurs autorités de protection des données cantonales. Les cantons de Fribourg, Vaud, Tessin et Zurich figuraient au programme de la visite.

Par la suite, nous allons concentrer nos activités sur la mise en place de contrôles du traitement des données personnelles dans le cadre du SIS, en particulier auprès de l'Office fédéral de la Police (maître du fichier N-SIS) et des services fédéraux utilisateurs du SIS, à l'instar des représentations suisses à l'étranger. De plus, nous allons développer notre rôle de coordinateur des autorités suisses de protection des données. A ce titre, nous assurons la présidence et le secrétariat du groupe de coordination, rassemblant le PFPDT et les autorités cantonales de protection des données. Nous avons institué ce groupe de coordination afin d'assurer une cohérence au niveau suisse entre les 27 autorités de protection des données par rapport aux demandes venant du Contrôleur Européen à la Protection des Données (CEDP) et afin de transmettre une information complète à toutes les autorités suisses rapidement et de manière coordonnée. Par ailleurs, en collaboration avec les autorités cantonales, nous allons élargir nos activités d'information et de sensibilisation du public aux enjeux en matière de protection des données dans le cadre de la mise en œuvre du SIS en Suisse. Nous projetons notamment d'élaborer des brochures à l'attention des utilisateurs du SIS et des personnes concernées par des traitements de données dans le cadre du SIS et de participer à une campagne d'information. Enfin, nous participons, avec les autorités cantonales de protection des données, à divers comités et groupes de travail internationaux. La Suisse délègue notamment deux représentants, le PFPDT et un représentant des autorités cantonales de protection des données, aux réunions de l'autorité de contrôle commune (ACC), chargée de surveiller la fonction de support technique central du SIS.

1.4.2 La lutte contre le hooliganisme

Dans le domaine de la lutte contre le hooliganisme, plusieurs travaux législatifs ont été poursuivis au cours de l'année écoulée. Dans ce contexte, nous avons été invités à prendre position sur divers projets qui se trouvaient à des stades très divers du processus législatif, du projet d'article constitutionnel aux directives régissant les traitements de données effectués par des personnes privées.

Diverses mesures prévues dans la loi fédérale sur les mesures visant au maintien de la sûreté intérieure (LMSI) et dans l'ordonnance qui s'y rapporte (OMSI) n'ont été mises en vigueur par le Parlement que pour une période limitée jusqu'à fin 2009. Ceci parce que la Confédération n'a pas le pouvoir de légiférer dans le domaine des mesures de

police de sécurité. Pour garantir que les dispositions correspondantes restent valables au-delà de la date indiquée, deux possibilités existent: d'une part, les cantons peuvent conclure un concordat dans lequel ils prévoient les mesures prévues ci-dessus. Les cantons ont choisi cette voie; elle pourrait cependant s'avérer plutôt laborieuse. Étant donné que le résultat est jusqu'à nouvel avis imprévisible, il est prévu d'autre part, en quelque sorte comme garantie supplémentaire, de formuler une nouvelle disposition dans la Constitution fédérale qui donnerait les compétences nécessaires à la Confédération. La différence entre les deux démarches est très importante sous l'angle des compétences. Cette question n'est cependant pas déterminante pour la protection des données, contrairement aux dispositions contenues dans les échelons législatifs suivants. C'est pourquoi nous nous sommes abstenus de prendre position sur le contenu du projet d'article constitutionnel, ce qui ne change bien sûr rien aux commentaires que nous avons faits sur les dispositions des niveaux inférieurs.

Nous mentionnons encore une fois notre critique envers la définition trop large de la notion de violence ainsi que notre constatation qu'une éventuelle utilisation de systèmes de reconnaissance faciale biométrique nécessite une disposition légale au sens formel et qu'une simple ordonnance ne suffit pas. La dernière constatation est notamment motivée par le fait que de tels systèmes servent à traiter non seulement les données des hooligans, mais en fait celles de toutes les personnes qui pénètrent dans le stade.

Pendant cette dernière période d'activité, nous avons également été invités à prendre position sur la directive relative à l'utilisation et au traitement de données issues du système d'information HOOGAN par les organisateurs de manifestations sportives et leurs responsables pour la sécurité. Nous avons éprouvé une grande satisfaction de constater qu'un grand nombre de questions avaient pu être éclaircies grâce à nos commentaires. Ceci vaut surtout pour la démarche appliquée lors de l'effacement des données sur place ou dans les stades. Nous avons également été ravis de prendre connaissance de la décision de ne pas mettre en place un système électronique de reconnaissance des personnes. Malheureusement, il existe un illogisme manifeste entre la disposition citée d'une part et la loi et l'ordonnance d'autre part, illogisme qui a été causé par l'article 2 al. 3 des directives. La formulation «Elles (les directives) s'appliquent par analogie aux retransmissions de manifestations sportives sur écran géant (projections publiques)» tend à étendre le champ d'application de la loi et de l'ordonnance au-delà de ce que dit le texte. Aussi bien la loi que l'ordonnance parlent de «manifestations sportives», ce qui dans le langage courant, n'inclut pas la retransmission de ces manifestations sur écran géant.

Il y a deux raisons qui font que cette situation n'est pas satisfaisante. Premièrement, une telle extension du champ d'application n'est pas possible du point de vue formel, et cela précisément dans le cadre de mesures entravant la liberté. Ceci est gênant dans la mesure où il sera nécessaire, en prévision de l'EURO 08, de prendre également des mesures de sécurité pour les projections publiques et qu'une certaine extension du champ d'application semble donc bienvenue. Deuxièmement, la formulation «par analogie» crée à notre avis des incertitudes puisqu'elle n'indique pas clairement ce que cela impliquera exactement en pratique. On peut par exemple s'attendre à des différences non négligeables du fait que les retransmissions sur écran géant ont généralement lieu sur le domaine public alors que la majorité des stades de football suisses sont en propriété privée. Une des différences qui pourraient se faire sentir est que le fait de pénétrer dans un stade malgré une interdiction de stade constitue une violation de domicile alors que la même situation sur le domaine public semble plutôt difficilement imaginable.

1.4.3 Activités en rapport avec l'EURO 08

L'EURO 08 va entraîner toute une série de traitements de données, effectués aussi bien par des autorités que par des particuliers. Nos activités dans ce cadre ont déjà été mentionnées dans nos rapports d'activités de ces deux dernières années. Au cours de l'année écoulée, nous avons reçu deux demandes.

La première demande concernait les directives régissant le traitement des images prises par des drones. Comme décrit dans notre dernier rapport d'activités (cf. 14ème rapport d'activités 2006/2007, ch. 1.3.5), nous avions assisté le DDPS lors de l'élaboration des règles citées. Bien que l'arrêté du Conseil fédéral à ce sujet n'ait pas été publié dans son intégralité, tous les éléments qu'il contient sont décrits dans le message relatif à l'arrêté fédéral sur l'engagement de l'armée en service d'appui en vue du soutien aux autorités civiles à l'occasion du Championnat d'Europe de football 2008 (UEFA EURO 2008). Ce qui importe surtout du point de vue de la protection des données est que le Conseil fédéral a, dans sa décision du 13 septembre 2006, autorisé l'engagement des moyens d'exploration des Forces aériennes «sous la condition qu'un enregistrement des données soit interdit» (FF 2006 7759, dernier alinéa avant l'art. 4).

La deuxième demande nous a été transmise par une personne qui n'avait pas reçu de billet lors du tirage au sort en mars 2007. Elle désirait savoir ce qui allait maintenant advenir de ses données et si elle avait éventuellement la possibilité de les faire supprimer. Les renseignements que nous avons pris auprès de l'UEFA ont établi que les don-

nées des requérants sont enregistrées dans une liste d'attente afin qu'elles puissent être réutilisées pour des tirages au sort ultérieurs. Les personnes concernées ont la possibilité de demander la suppression de leurs données, mais l'UEFA exige, selon les informations sur son site web, pour cela qu'elles fassent une demande écrite. L'utilité de la liste d'attente découle des diverses possibilités qui existent que quelqu'un obtienne un billet après coup, même s'il n'en a pas reçu lors du tirage au sort. De tels cas peuvent se produire (1) lorsqu'une personne n'a pas payé pour un billet qui lui a été attribué; (2) lorsqu'une personne qui a été tirée au sort doit être exclue pour des raisons de sécurité parce qu'elle figure sur une liste de personnes ayant commis des actes de violence ou (3) si une association nationale ne devait pas épuiser son contingent dans une partie de la phase KO pour laquelle les équipes participantes ne sont actuellement pas encore connues. À la fin du championnat, toutes les données de requérants qui ne doivent pas être conservées pour des raisons juridiques sont supprimées. Selon l'UEFA, cela concerne d'une part les cas où l'on a encore besoin des informations pour des raisons fiscales, d'autre part, les cas où les données sont encore utilisées dans le cadre de litiges juridiques ou d'incidents ayant compromis la sécurité.

1.4.4 Loi fédérale sur les systèmes d'information de police de la Confédération

Le Conseil national a adopté le projet de loi fédérale sur les systèmes d'information de police de la Confédération. Les propositions que nous avons émises sur de nombreux points du projet n'ont toutefois pas été retenues. En ce qui concerne la question particulière du droit d'accès dit «indirect», la réglementation adoptée a été proposée par le Département fédéral de justice et police et l'Office fédéral de la police. Cette réglementation constitue une amélioration par rapport à la situation actuelle qui n'est pas conforme à l'article 13 de la Constitution fédérale et aux articles 8 et 13 de la Convention européenne des droits de l'homme qui garantissent la protection de la sphère privée. Cependant, nous ne sommes pas satisfaits que l'information de la personne concernée soit différée automatiquement de trois ans lorsque celle-ci n'est pas enregistrée.

Nous avons mentionné dans notre 14ème rapport d'activités 2006/2007 (ch. 1.3.7) un certain nombre de remarques sur le projet de loi fédérale sur les systèmes d'information de police de la Confédération. En premier lieu, nous avons regretté le maintien du système dit du «droit d'accès indirect». Nous avons également critiqué le fait qu'une information ultérieure des personnes concernées n'est prévue que lorsque les don-

nées ont été recueillies directement (et à leur insu) par la Police judiciaire fédérale. Nous avons de plus exprimé des doutes quant à l'accès en ligne de la Commission fédérale des maisons de jeu au système de recherche informatisée de police ainsi que celui du Bureau de communication en matière de blanchiment d'argent au système de traitement des données relatives à la protection des données (ISIS). Nous nous sommes finalement opposés à la mention dans l'index national de police du motif de l'inscription lorsqu'une personne fait l'objet d'un relevé signalétique ainsi qu'à la désignation du système d'information ou du type de système d'où proviennent les données. Le projet de loi a été examiné par le Conseil national et celui-ci a adopté un texte qui ne tient pas compte de nos diverses remarques.

Dans le cadre des travaux de la Commission des affaires juridiques du Conseil national, une nouvelle réglementation concernant l'accès par la personnes concernées aux données contenues dans le système de traitement des données relatives aux infractions fédérales a été élaborée. Ces données sont actuellement traitées dans le fichier JANUS de la Police judiciaire fédérale. Cette nouvelle réglementation a été proposée par le Département fédéral de justice et police et l'Office fédéral de la police (fedpol). Une personne peut demander si des données la concernant sont traitées par la Police judiciaire fédérale dans le système d'information susmentionné. Fedpol ajourne le renseignement si les données traitées sont liées à des intérêts prépondérants pour la poursuite pénale qui exigent le maintien du secret. Le renseignement est également ajourné si la personne n'est pas enregistrée. Fedpol communique à la personne concernée l'ajournement du renseignement et l'informe du fait qu'elle peut demander au PFPDT qu'il vérifie si des données la concernant sont traitées conformément au droit et si des intérêts prépondérants liés au maintien du secret justifient l'ajournement. Sur demande de la personne concernée, le PFPDT effectue la vérification et lui communique une réponse selon laquelle aucune donnée la concernant n'est traitée illégalement ou que, dans le cas d'une erreur dans le traitement des données ou concernant l'ajournement du renseignement, il a adressé à fedpol la recommandation d'y remédier. Le préposé indique également à la personne concernée qu'elle peut demander au Tribunal administratif fédéral (TAF) qu'il examine la communication ou l'exécution de la recommandation émise. Sur demande de la personne concernée, le TAF effectue la vérification puis lui communique qu'il l'a menée conformément au sens de la requête. En cas d'erreurs dans le traitement des données ou concernant l'ajournement du renseignement, le TAF adresse à l'office une décision lui demandant d'y remédier. La procédure est la même lorsque la recommandation du préposé n'est pas observée. Celui-ci peut porter un recours contre cette décision devant le Tribunal fédéral. Les communications susmentionnées sont toujours libellés de manière identique et sans justification. Elles ne peuvent pas faire l'objet d'un recours. Fedpol

communique les renseignements aux personnes qui les ont demandés dès lors que les intérêts liés au maintien du secret ne peuvent plus être invoqués, mais au plus tard après expiration du délai de conservation, pour autant que cela n'entraîne pas un volume de travail excessif. Les personnes au sujet desquelles aucune donnée n'a été traitée en sont informées par l'office trois ans après réception de leur demande. Si une personne rend vraisemblable que l'ajournement du renseignement la lèse gravement et de manière irréparable, le préposé peut recommander que l'office fournisse immédiatement le renseignement à titre exceptionnel, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure.

Cette nouvelle réglementation constitue certes une amélioration par rapport à la situation actuelle qui n'est pas conforme à l'article 13 de la Constitution fédérale et aux articles 8 et 13 de la Convention européenne des droits de l'homme qui garantissent la protection de la sphère privée. Nous ne sommes par contre pas satisfaits que l'information de la personne concernée soit différée automatiquement de trois ans lorsque celle-ci n'est pas enregistrée. Dans la plupart des cas, il n'y a pas de risque particulier pour la sécurité intérieure et extérieure de l'informer immédiatement de cette situation. Si un délai général devait être introduit, il ne devrait pas dépasser six mois. Le projet est actuellement examiné par le Conseil des Etats.

1.4.5 Surveillance par vidéo de lieux publics en vue d'assurer la sécurité

Un rapport a été rédigé sous la direction du DFJP concernant la surveillance de sécurité des lieux publics par caméra vidéo. Nous avons accompagné ces travaux en qualité d'observateurs. En ce qui concerne la prolongation de la durée de conservation proposée dans le rapport, nous avons relevé que le principe de la proportionnalité devait être respecté. Nous avons également critiqué le fait que le rapport ne rendait pas suffisamment compte des inconvénients et des risques d'une surveillance par vidéo.

Un rapport a été rédigé sous la direction du DFJP concernant la surveillance de sécurité des lieux publics par caméra vidéo. Nous avons accompagné ces travaux en qualité d'observateurs. Une des principales conclusions de ce rapport est que la durée de conservation des enregistrements vidéo, qui est de 24 heures pour le Service fédéral de sécurité, est trop courte. On propose dès lors de modifier la base légale correspondante. Lors des séances ainsi que dans notre prise de position sur le projet de rapport, nous avons retenu qu'une éventuelle prolongation de la durée de conservation pour le Service fédéral de sécurité devait être conforme aux principes généraux de la

protection des données, en particulier au principe de proportionnalité. Ainsi, une prolongation de la durée à 100 jours serait en tous les cas disproportionnée. Nous avons également relevé que le rapport était, dans son ensemble, trop partial dans le sens qu'il mentionnait surtout les avantages d'une surveillance par vidéo et ne parlait pas des risques qu'une telle surveillance présente. Une surveillance par vidéo peut certainement être judicieuse et utile dans certains cas. Elle ne permet cependant pas d'empêcher complètement la criminalité, celle-ci étant souvent simplement déplacée en d'autres endroits. D'autre part, une telle surveillance a souvent pour effet d'améliorer le sentiment de sécurité des personnes surveillées, mais pas la sécurité en soi. Avant d'engager des appareils de vidéosurveillance et de créer les bases légales correspondantes, il y a lieu d'examiner consciencieusement de cas en cas si les exigences de la protection des données (telles que le principe de la proportionnalité et celui de la finalité) sont respectées. On vérifiera en particulier s'il n'est pas possible d'atteindre le même objectif avec une mesure moins radicale que la surveillance vidéo. D'autre part, la vidéosurveillance doit être accompagnée de certaines mesures (telles que la destruction des enregistrements dès que ceux-ci ne sont plus utilisés, l'utilisation de technologies respectueuses de la protection des données.

1.4.6 Accord entre la Suisse et la France relatif à la coopération transfrontalière en matière judiciaire, policière et douanière

L'accord révisé avec la France relatif à la coopération transfrontalière en matière judiciaire, policière et douanière renforce la protection des données par rapport à l'accord initial de 1998. Les dispositions de protection des données de cet accord révisé sont similaires à celles de l'accord avec l'Allemagne et de l'accord avec l'Autriche et le Liechtenstein.

Les dispositions relatives à la protection des données de l'accord révisé dans le courant 2007 sont plus complètes que celles de l'accord initial de 1998 et renforcent ainsi la protection des données personnelles traitées dans le cadre de la coopération transfrontalière en matière judiciaire, policière et douanière avec la France. Elles reprennent en partie les normes de la Convention d'application de Schengen et s'inspirent des dispositions de protection des données contenues dans l'accord avec l'Allemagne et dans l'accord avec l'Autriche et le Liechtenstein. Ces dispositions traitent de la finalité du traitement des données personnelles, de la rectification, de la destruction ainsi que de la communication de ces données. L'accord révisé contient également une disposition sur le droit d'être renseigné.

Dans le cadre de l'élaboration du projet d'accord révisé, nous avons été contactés à plusieurs reprises par l'Office fédéral de la police. Celui-ci a tenu compte de toutes nos remarques, notamment de la nécessité de mentionner dans l'accord qu'un protocole additionnel règlera le contrôle de la base de données commune utilisée par les agents des centres de coopération policière et douanière. En effet, il est important de définir les compétences des différentes autorités de protection des données (Commission Nationale de l'Informatique et des Libertés, PFPDT et autorités cantonales de protection des données) selon que ce dont les autorités françaises ou suisses (autorités fédérales et cantonales) qui sont actives dans ces centres communs.

1.4.7 Le droit d'accès indirect

En vertu des articles 18, alinéa 2, de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) et 14, alinéa 3, de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC), le Président de la Cour I du Tribunal administratif fédéral (TAF), compétente en matière de protection des données, examine à la demande de la personne concernée la communication du PFPDT ou l'exécution, le cas échéant de la recommandation émise par ce dernier. Par la suite, le Président communique à la personne concernée une réponse au libellé toujours identique selon lequel l'examen a eu lieu conformément au sens de la requête. Depuis le 1er janvier 2007, le TAF a repris les tâches de la Commission fédérale de la protection des données et de la transparence dans le domaine du droit d'accès indirect.

Nous avons organisé en collaboration avec le Tribunal administratif fédéral et sur sa requête - une séance d'information sur les différents aspects de la procédure relative au droit d'accès indirect pour les personnes chargées du traitement des demandes déposées en vertu des articles 18 LMSI et 14 LOC. Le Président de l'ancienne Commission fédérale de la protection des données et de la transparence a également participé à cette séance d'information.

Dans le cadre de l'examen du projet de loi fédérale sur les systèmes d'information de police de la Confédération par la Commission des affaires juridiques du Conseil national, de nouvelles modalités pour l'exercice du droit d'accès ont été retenues. Des informations plus détaillées sur cette question se trouvent au chiffre 1.4.4.

1.4.8 Information ultérieure des personnes concernées

Le DFJP est d'avis que sa décision du 15 août 2006 sur l'information ultérieure des personnes concernées dans le domaine policier n'est pas une décision au sens propre. Celle-ci ne doit pas par conséquent être publiée. Nous avons invité le DFJP à prendre une décision au sens de l'art. 5 PA et de la publier sous une forme anonymisée. Le DFJP examine actuellement si avons la compétence d'exiger une telle décision.

Dans notre dernier rapport d'activités, nous avions déjà mentionné la décision du DFJP du 15 août 2006 relative à l'information ultérieure des personnes concernées dans le domaine policier ainsi que nos recommandations correspondantes (cf. notre 14ème rapport d'activités 2006/2007, ch. 1.3.8). La décision prévoyait entre autres qu'un extrait soit publié dans la Feuille fédérale. Nous défendions par contre le point de vue qu'il fallait publier l'intégralité (anonymisée) de la décision, ou à défaut, un extrait contenant les éléments essentiels en indiquant les voies de recours. Le DFJP, de son côté, défendait le point de vue que sa décision ne constituait pas une décision au sens de l'article 5 de la loi fédérale sur la procédure administrative (PA), mais qu'il s'agissait d'une mesure interne ne justifiant pas une publication. Nous n'avions pas partagé cette interprétation et continué à exiger du DFJP qu'il publie la décision. Si le DFJP devait continuer à faire valoir qu'il ne s'agit pas là d'une décision au sens de l'article 5 PA, il doit à notre avis prendre une telle décision et la publier sous forme anonymisée dans la Feuille fédérale ainsi que sur son site web. Le DFJP examine actuellement si nous avons la compétence d'exiger une telle décision.

1.5 Santé

1.5.1 Création de profils d'ADN dans le cadre de regroupements familiaux

L'introduction dans la loi française sur l'immigration de tests d'ADN pour les membres d'une famille qui rejoignent leurs parents a provoqué des discussions très animées. En Suisse, cette pratique existe déjà: dans des cas exceptionnels, la délivrance d'une autorisation peut être subordonnée à une analyse génétique, pour autant que la personne concernée donne son accord par écrit. A notre avis, cette pratique doit cependant être appliquée de manière extrêmement restrictive.

Le 1er avril 2007, la loi fédérale sur l'analyse génétique humaine (LAGH) est entrée en vigueur. Celle-ci permet, dans le cadre d'une procédure administrative, de subordonner l'octroi d'une autorisation ou de prestations à l'établissement d'un profil d'ADN si la filiation ou l'identité d'une personne font l'objet de doutes fondés qui ne peuvent être levés d'une autre manière. Ces profils d'ADN ne peuvent être établis qu'avec le consentement écrit des personnes concernées.

Il doit donc s'agir de cas d'exception dont la clarification au moyen de profils d'ADN doit être faite en respectant le principe de la proportionnalité. C'est par exemple le cas lorsqu'on est en présence d'actes d'état civil provenant de pays qui ont des offices d'état civil peu développés et parfois pas très fiables.

Lors d'une demande de regroupement familial, l'analyse génétique peut être limitée à la relation entre la mère et l'enfant afin d'éviter des tragédies familiales. Il existe un nombre non négligeable d'enfants qui sont nés d'une union conjugale et ont donc comme père légal l'époux de leur mère, mais dont le père génétique est un autre homme.

Les discussions menées en France ont également lancé un débat en Suisse. Ainsi, le conseiller national Carlo Sommaruga a demandé dans une motion du 5 octobre 2007 au Conseil fédéral de présenter un rapport sur l'utilisation de tests d'ADN dans le cadre du regroupement familial. Nous avons soutenu cette motion, car nous sommes d'avis qu'un rapport serait très utile dans ce domaine complexe et délicat. De son côté, le conseiller national Alfred Heer a déposé une initiative parlementaire demandant qu'un test d'ADN soit obligatoire pour les regroupements de familles en provenance de pays à problèmes.

Du point de vue de la protection des données, une analyse génétique doit être proportionnelle et donc ordonnée en ultime recours. Le caractère libre de l'analyse est relatif vu que le requérant risque de ne pas recevoir de visa s'il refuse de donner son consentement. Il doit en outre supporter les frais de cette analyse.

Contrairement à la Suisse, les analyses génétiques en France sont ordonnées par un juge et payées par l'État. La base légale permettant d'ordonner une analyse génétique en Suisse est donnée avec la LAGH.

1.5.2 La transmission d'échantillons biologiques vers les États-Unis dans le cadre de la recherche médicale

Un échantillon biologique peut être exporté vers les États-Unis à condition que la personne concernée ait préalablement donné son consentement. Si ce consentement fait défaut, l'échantillon ne peut être transmis que si l'on a des garanties que le pays destinataire dispose d'une protection des données adéquate.

La législation actuelle suisse concernant la recherche sur l'être humain (c.-à-d. aussi bien sur des personnes que sur des matériels biologiques humains) est malheureusement encore lacunaire. Avec deux motions, le Parlement a chargé le Conseil fédéral de réglementer ce domaine par un article constitutionnel et une loi fédérale relative à la recherche sur l'être humain (cf. notre 14ème rapport d'activités 2006/2007, ch. 1.4.1). Pour l'instant, les seules réglementations qui existent au niveau fédéral concernent des domaines médicaux spécifiques, notamment les essais cliniques avec des médicaments. De plus en plus fréquemment, des échantillons biologiques sont envoyés à l'étranger, notamment aux Etats-Unis, pour y être analysés.

La transmission d'échantillons biologiques à l'étranger présente un risque accru d'atteinte à la personnalité des personnes concernées. En l'absence de réglementations légales spéciales, tout traitement de données personnelles, donc aussi la transmission d'échantillons biologiques à l'étranger, est soumis à la loi sur la protection des données (LPD).

La loi révisée sur la protection des données, qui est entrée en vigueur le 1er janvier 2008, exige, pour une communication de données à l'étranger, que la législation en matière de protection des données du pays destinataire offre une protection adéquate. Contrairement aux pays membres de l'Union européenne, ceci n'est pas le cas aux États-Unis. Dans les cas où une protection adéquate fait défaut, des garanties suffisantes doivent être obtenues que la communication de données ne menace pas gravement la personnalité des personnes concernées. Ces garanties peuvent être

fixées dans un contrat (dispositions de protection des données) ou résulter d'un code de conduite. Un exemple d'un ensemble de règles auquel des personnes privées peuvent se soumettre volontairement est le «Safe Harbor Privacy Framework», qui a été négocié entre la Commission européenne et les États-Unis. Il faut toutefois relever que quiconque se base sur de telles garanties reste néanmoins lui-même responsable de protéger les données et doit nous informer des garanties reçues.

Dans des cas particuliers, une communication est également possible si la personne concernée a donné son consentement. Ce consentement doit avoir été donné librement et de manière explicite, ce qui signifie que la personne concernée doit savoir quelles données la concernant ont été communiquées à quelle fin et à quel destinataire. Elle doit également être informée de l'absence d'une protection adéquate des données.

1.5.3 Echange international de données dans la lutte contre le dopage

L'Agence mondiale antidopage (AMA) a pour tâche de coordonner et de superviser les mesures de lutte contre le dopage. Des données étant dans ce contexte aussi collectées en Suisse, nous avons analysé les activités de l'Agence qui pourraient être concernées par la loi suisse sur la protection des données (LPD). Nous sommes arrivés à la conclusion que la soumission de l'AMA à la LPD ne peut, dans des domaines partiels, être exclue. Dans le cadre de la révision de la loi sur l'encouragement du sport, nous avons donc suggéré la création d'une base légale permettant de simplifier la coopération internationale dans la lutte antidopage.

Dans la lutte antidopage, l'AMA assume trois tâches principales. Elle est tout d'abord l'organe central de gestion des données et des résultats des tests antidopage, au niveau international et aux différents niveaux nationaux. Dans ce cadre, tous les tests des sportifs qui lui sont assignés pendant et en dehors d'une compétition lui sont annoncés. La seconde mission importante de l'AMA est l'organisation indépendantes de tests de dopage ainsi que leur coordination. En troisième lieu, l'AMA gère une banque de données centrale dans laquelle sont introduits les profils de personnalité de tous les sportives et sportifs enregistrés auprès d'elle (y compris leurs antécédents en matière de santé et de dopage). Nous avons analysé en détail ces trois domaines d'activités dans le cadre d'une expertise rédigée pour l'AMA, en raison de notre compétence et de la soumission de l'AMA à la loi suisse sur la protection des données.

L'application de la LPD et, de ce fait, la compétence du PFPDT sont soumises au principe de la territorialité. Cela signifie que la LPD n'est applicable que pour un traitement de données qui a lieu en Suisse. Si toutefois le traitement de données touche un contexte international, la personne concernée a, en vertu de la loi fédérale sur le droit international privé (LDIP), la possibilité de choisir entre le droit de l'Etat dans lequel l'auteur de l'atteinte a son établissement ou sa résidence habituelle et le droit de l'Etat dans lequel le résultat de l'atteinte se produit, pour autant que l'auteur du dommage ait dû s'attendre à ce que le résultat se produise dans cet Etat. Ainsi la possibilité que la personne traitant des données pourrait se procurer des avantages en transposant son siège social à l'étranger et en se soumettant ainsi à un autre ordre juridique est dans une large mesure supprimée. Dans ce contexte, il s'agissait dans les trois domaines d'activités mentionnés plus haut d'examiner si et dans quelle mesure l'AMA est soumise à la LPD.

Dans le cadre de sa fonction en tant qu'organe central, l'AMA est informée par les organisations antidopage nationales (par ex. en Suisse) des données personnelles sensibles (en général les résultats des contrôles) transférées au Canada. Selon la LPD, ce type de transfert n'est possible que si la législation du pays étranger offre un niveau de protection des données adéquat ou si elle est en mesure de garantir d'une autre manière un niveau adéquat. L'AMA étant une fondation non commerciale et la loi canadienne sur la protection des données n'offrant pas de protection adéquate pour les institutions non commerciales, les organisations suisses antidopage envisageant une transmission de données vers le Canada doivent veiller elles-mêmes à assurer un niveau de protection des données adéquat, par exemple au moyen d'une convention avec l'AMA. Par contre, le transfert de données dans l'autre sens, à savoir du Canada vers la Suisse, n'est pas soumis au régime suisse de protection des données.

Les contrôles de dopages effectués par l'AMA impliquent le traitement de données personnelles; ses contrôles effectués en Suisse sont donc soumis à la législation suisse sur la protection des données.

Etant donné que l'AMA exploite sa banque de données électronique (ADAMS) uniquement au Canada et que les processus de traitement qu'elle effectue n'ont pas lieu en Suisse, l'exploitation de l'ADAMS n'est pas soumise à la législation suisse sur la protection des données.

Dans le cadre de notre examen, il nous est apparu d'une manière générale qu'on ne peut exclure dans tous les cas une soumission de l'AMA à la législation suisse sur la protection des données. Dans le but de simplifier la coopération internationale en matière de contrôle du dopage et de transfert de données au niveau international

dans le cadre de la lutte antidopage, nous avons donc profité de la révision de la loi sur l'encouragement du sport pour suggérer de créer une base légale appropriée (cf. également à ce sujet le chiffre 1.5.4).

1.5.4 Révision de la loi fédérale encourageant la gymnastique et les sports

Actuellement, le transfert international de données dans le but de lutter contre le dopage ainsi que l'organisation de contrôles antidopage ne sont pas réglés par le droit suisse, ce qui se traduit souvent pour les acteurs impliqués par une insécurité du droit. Du fait de l'absence de base juridique, les différents organes de lutte antidopage ne peuvent aujourd'hui procéder au niveau international à un échange de données que si une protection adéquate des données est garantie par contrat ou par la loi. D'autre part, d'un point de vue strictement juridique, les contrôles antidopage en Suisse reposent sur un accord volontaire du sportif concerné, qu'il donne sous forme de déclaration. Cette pratique est contestée car un refus mène à l'exclusion de la manifestation et que dans ces conditions il ne peut être question de consentement. Afin d'aborder ces deux problématiques, nous avons déposé deux propositions d'adaptation législative dans le cadre de la révision de la loi sur l'encouragement du sport.

L'efficacité de la lutte contre le dopage au niveau international dépend en grande partie de l'échange de données entre les différents organes nationaux antidopage. Or, aujourd'hui en Suisse, il n'existe toujours pas de norme légale en ce qui concerne la coordination des mesures de lutte antidopage (organisation de contrôles) et la communication des cas de dopage. Ce sont donc les règles générales de la loi sur la protection des données (LPD) qui sont applicables. De ce fait, la transmission transfrontière de ces données personnelles sensibles peut générer des situations difficiles lorsque ces données sont communiquées à un Etat qui n'offre pas de protection des données adéquate. Pour remédier à ces difficultés, on peut concevoir que les organes nationaux antidopage des pays participant à l'échange de données concluent entre eux des accords. Mais comme dans la pratique, la négociation d'un grand nombre d'accords est longue et compliquée, nous avons suggéré de créer une base légale appropriée. Conformément à cette base qui a été admise lors de la procédure de consultation relative à la loi sur l'encouragement du sport, les services compétents seraient habilités à échanger des données personnelles avec des organes reconnus étrangers et internationaux à des fins de lutte contre le dopage, lorsque les contrôles

antidopage, leur coordination ou la communication de cas de dopage le requièrent. Ce projet de réglementation a pour but, en particulier pour les organes nationaux de lutte contre le dopage, de créer une sécurité juridique et de leur faciliter la tâche.

Les contrôles antidopage reposent actuellement sur une déclaration de consentement des sportifs. Mais si ceux-ci refusent de remettre ce genre de déclaration ou de se soumettre à un contrôle, cela conduit dans la pratique actuelle du sport de compétition soit à une exclusion de la compétition, soit à la perte de la licence sportive. Or, le consentement donné par les sportifs pour les contrôles et le traitement de données qui s'ensuit ne peut à notre avis être considéré comme un consentement libre. Pour cette raison, nous avons suggéré de créer une base légale légitimant les contrôles antidopage. Notre proposition d'adaptation législative selon laquelle les sportifs qui participent régulièrement à des compétitions peuvent être tenus de se soumettre en tout temps à des contrôles antidopage, a été intégrée au projet de révision de la loi sur l'encouragement du sport. Cela devrait permettre de créer une sécurité du droit pour les sportifs et les organisateurs, également dans le domaine des contrôles antidopage.

1.5.5 Exigences de la protection des données pour les autorisations générales délivrées pour la recherche médicale

Lorsqu'un hôpital est en possession d'une autorisation générale de la Commission d'experts pour le secret professionnel dans la recherche médicale, il est tenu de respecter les contraintes qui lui ont été imposées. Des mécanismes de contrôle doivent être mis en place; leur utilisation n'est pas limitée à la vérification de la demande pour le projet de recherche, mais ils doivent plutôt être intégrés dans le projet de recherche sous une forme technique et organisationnelle appropriée.

Une procédure d'autorisation simplifiée est prévue pour les organisations, telles que les hôpitaux, qui travaillent sur un grand nombre de projets de recherche, afin d'éviter qu'il faille demander une autorisation spéciale pour chaque projet de recherche. Cette autorisation générale doit être demandée auprès de la Commission d'experts. Elle est valable pour une durée de 5 ans et peut être renouvelée. Cette autorisation donne le droit aux chercheurs et aux doctorants de l'institution concernée d'utiliser des données de patients pour la recherche interne à l'institution.

Le détenteur de l'autorisation doit mettre en place des mécanismes de contrôle qui permettent de garantir une protection efficace des données des patients. Ces mécanismes ne sont pas seulement importants pour l'examen et l'autorisation du projet

interne, ils doivent également être appliqués au sein du projet de recherche même afin de permettre de vérifier après coup si les charges assorties par la Commission d'experts ont été respectées.

Aujourd'hui, les hôpitaux utilisent des archives papier ou un système d'archivage électronique dans lesquels les données des patients sont enregistrées environ deux semaines après que ceux-ci ont quitté l'établissement. Dans la majorité des cas, les chercheurs utilisent ces données archivées pour leurs recherches. C'est surtout dans ce domaine que les exigences d'ordre technique et organisationnel de la commission d'experts doivent être documentées et appliquées. Le processus complet de la saisie des données archivées (y compris la journalisation) jusqu'à leur suppression doit y être indiqué. Il convient de démontrer à l'aide de quelles informations et quels collaborateurs le chercheur peut accéder aux données, quelles sont les données qu'il extrait et quand et comment il les anonymise ou pseudonymise. Il convient également d'indiquer quels moyens matériels le chercheur utilise pour traiter les données dans le cadre de son projet de recherche et comment il les sauvegarde, dans le cas où elles ne sont pas complètement anonymisées (si les données sont anonymisées, les exigences de la protection des données ne sont plus applicables). La plupart du temps, les données collectées sont utilisées de manière pseudonymisée, il y a donc lieu d'indiquer également comment ces données peuvent être réattribuées et comment ce processus peut être contrôlé.

Le domaine médical traite des données personnelles sensibles, c'est pourquoi les exigences d'ordre normatif demandent que celles-ci soient protégées selon l'état de la technique. Pour les travaux de recherche effectués sur la base de données archivées sous forme papier, nous considérons notamment la démarche ci-dessous comme adéquate:

- Les dossiers papier demandés par le chercheur lui sont remis par un collaborateur des archives qui consigne dans un journal quels dossiers il a mis à disposition du chercheur.

- En règle générale, le chercheur transfère ces données sur un ordinateur portable. Il doit veiller lors de ce transfert à ce que les données soient reprises sous une forme pseudonymisée, à moins qu'elles aient déjà été anonymisées à l'origine. D'autre part, les données identifiantes attribuées au pseudonyme utilisé ne doivent pas se trouver en clair sur l'ordinateur portable. Elles doivent être protégées par un cryptage efficace ou, encore mieux, ne pas du tout être stockées sur l'ordinateur portable. Le transfert sur l'ordinateur portable des informations en provenance des dossiers devrait si possible se faire dans les

locaux des archives. Pour plus de sécurité, nous recommandons également de ne pas connecter l'ordinateur portable à un réseau de communication pendant toute la durée des travaux de recherche.

Pour les travaux de recherche effectués avec des données stockées dans une base de données, ces considérations sont également applicables. Lors de la conception des grilles d'écran et des listes imprimées il faut partir du principe que seules les données absolument nécessaires pour le traitement doivent être traitées. Pour autant que le chercheur ne doive pas entrer en contact avec les patients, il suffira de veiller à ce qu'il travaille avec des données anonymisées ou des pseudonymes. On peut ainsi envisager qu'une clinique mette sur pied plusieurs comptes qui seraient mis à disposition des chercheurs pour leurs travaux. Dans les cas où les chercheurs peuvent interroger eux-mêmes les bases de données, il n'est à notre avis pas nécessaire d'impliquer les collaborateurs des archives. Si les traitements concernent des données de personnes identifiées ou identifiables, une telle démarche nécessite cependant que les accès soient dûment journalisés sous une forme si possible pseudonymisée et satisfaisant aux exigences de la révision.

Lors de nos visites sur place, nous avons également constaté que non seulement les chercheurs, mais aussi les médecins pouvaient, dans le cadre de leur travail quotidien, accéder au système d'archivage électronique. Cet accès est notamment nécessaire pour constater si un patient nouvellement admis à l'hôpital y a déjà été soigné une fois et si les archives contiennent éventuellement des informations importantes sur ce patient. Un moyen possible de contrôler cet accès à la base de données en fonction de l'accomplissement de la tâche serait de n'autoriser l'accès que si le patient a déjà été enregistré dans le système d'admission des patients. Un tel mécanisme de contrôle d'ordre préventif permettrait déjà de réglementer de manière relativement satisfaisante l'accès à la base de données pour le travail quotidien. Le système doit en outre être conçu de manière à ce qu'il permette l'accès à la base de données d'archives en cas d'urgence. D'autre part, tous les accès à des données personnelles sensibles doivent être journalisés selon les critères indiqués ci-dessus.

Nous estimons également important de mentionner que la fonction de conseil en matière de protection des données dans un hôpital est une tâche essentielle qui ne peut pas être assumée en y consacrant 10 % du temps de travail. La personne qui assume cette tâche doit non seulement faire preuve de ténacité, mais elle doit également disposer de vastes connaissances. Nous insistons régulièrement sur le fait que pour assumer correctement les tâches qui lui sont confiées, cette personne doit notamment avoir des connaissances de base dans les domaines suivants: informatique, organisation, gestion d'entreprise, sécurité de l'information, didactique et droit.

1.5.6 Projets de recherche médicale se fondant sur le consentement des personnes concernées

Le consentement d'un patient n'est valable que si celui-ci a été suffisamment informé pour pouvoir se faire une image claire du traitement de données prévu. Le consentement doit être donné de plein gré et peut donc uniquement être demandé si la personne concernée n'est pas contrainte ou mise sous pression.

En principe, la recherche médicale n'est autorisée à utiliser les données d'un patient que si ce dernier – ou, selon la situation, son représentant légal ou un proche parent – a donné son consentement. Si le consentement ne peut pas être obtenu, l'institution a la possibilité de demander auprès de la Commission d'experts pour le secret professionnel dans la recherche médicale une autorisation pour ce projet de recherche.

Pour les projets de recherche qui ont lieu avec le consentement des personnes concernées, les critères suivants doivent notamment être respectés:

Le consentement d'un patient n'est valable que s'il a été donné librement et que la personne concernée a été suffisamment informée. Le caractère libre du consentement n'existe que si la personne concernée n'a pas été contrainte ou mise sous pression. Cela signifie par exemple que l'on ne demandera pas le consentement d'un patient juste avant que celui-ci subisse une opération importante, mais plutôt après l'opération, pour éviter de mettre le patient sous pression. Le patient a en outre le droit de révoquer en tout temps son consentement, toutefois uniquement avec effet dans le futur.

La personne concernée est considérée comme suffisamment informée si elle sait à l'avance quelles données la concernant seront traitées par quels organes à quelles fins et de quelle manière. Elle doit également être informée sur les mesures organisationnelles et techniques qui ont été prises pour protéger les données. L'information du patient doit débuter lors de la collecte des données et ne se termine qu'une fois que les données ont été détruites ou anonymisées. Si, sur la base des informations qu'elle a reçue, la personne concernée se fait une fausse image de la nature, de l'envergure et du but du traitement de données, le consentement est considéré comme nul et non avenu et le traitement de données comme contraire à la loi.

1.6 Assurances

1.6.1 La mise en œuvre de la cinquième révision de l'AI

La loi révisée sur l'assurance-invalidité (LAI) et l'ordonnance qui s'y rapporte (RAI) sont entrées en vigueur le 1er janvier 2008. Le modèle de la détection précoce des cas d'invalidité en est l'une des principales innovations. La réglementation des mesures de détection précoce nécessite, sous l'angle de la protection des données, un certain nombre d'améliorations.

Les questions de protection des données relatives à la révision de la loi sur l'assurance-invalidité ont été déjà discutées au cours des années précédentes (cf. notre 13ème rapport d'activités 2005/2006, chiffre 5.1.2). Il ne restait encore à examiner que la concrétisation de la loi au niveau de l'ordonnance. Nous nous sommes prononcés à ce sujet dans le cadre de la consultation des offices.

La réglementation de la compétence relative aux annonces en cas d'atteintes à la santé invalidantes a donné lieu à certaines critiques. Ce genre d'annonce peut avoir lieu non seulement si l'employé a présenté une incapacité de travail ininterrompue de 30 jours, mais aussi lorsqu'une personne s'absente, pour des raisons de santé, de manière répétée pour des périodes de courte durée pendant une année (art. 1ter, al. 1, let. b, RAI). A la différence d'une absence d'un mois, le fait d'être absent de son poste de travail à plusieurs reprises au cours d'une même année en raison de problèmes de santé n'est pas inhabituel au point que le risque d'invalidité serait manifeste. Donc, dans ce cas, l'annonce d'une personne auprès de l'AI repose plus fortement sur des indices que ce n'est le cas pour une absence de 30 jours.

Ce scepticisme au niveau de la protection des données est né du souci d'exactitude des données: le principe de l'exactitude ne signifie pas seulement qu'il faut enregistrer des données correctes, mais aussi que dans la mesure du possible un traitement de données ne repose pas sur un simple soupçon. Il convient néanmoins d'admettre dans ce contexte que les efforts légitimes déployés en matière de prévention des risques impliquent nécessairement la vérification des soupçons. En tout état de cause, le législateur doit ici s'efforcer de donner une description aussi précise que possible de ce qu'est l'indice ou le soupçon déterminant. Nous avons donc plaidé pour que le cas des absences brèves mais répétées soit défini avec plus de précision, par l'indication d'un nombre minimum de jours de maladie par année civile. L'OFAS, en sa qualité d'office responsable, a cependant refusé de souscrire à cette requête.

1.6.2 La nouvelle réglementation du Système central d'information (ZIS)

Le système central d'information des assureurs (ZIS) élaboré en vue de lutter contre les fraudes dans le domaine des assurances a déjà fait l'objet de nos commentaires dans de précédents rapports d'activités. Ces prises de position ont quelque peu perdu de leur actualité depuis que le règlement du ZIS a été remanié. Mais toutes les réserves du point de vue de la protection des données n'ont pas été écartées à ce jour.

Le système central d'information (ZIS) est un instrument important dans la lutte contre les manœuvres frauduleuses dans le domaine des assurances. Il a été annoncé en 1995 auprès du PFPDT (à l'époque PFPD) en tant que fichier et doit aujourd'hui faire l'objet d'une révision. Les organes responsables du ZIS nous ont soumis le nouveau règlement. Les deux modifications qui nous ont paru essentielles sont l'amélioration de la transparence et la révision des critères pour une inscription dans le système.

Nous avons expressément approuvé l'amélioration de la transparence. Par contre, nous avons exprimé des réserves quant à la nouvelle réglementation des motifs d'enregistrement dans le système. Pour la raison suivante: désormais, les cas dans lesquels les soupçons n'ont pas été encore confirmés par le jugement d'un tribunal devront aussi être saisis dans la banque de données centrale.

Du point de vue de la protection des données, un traitement de données reposant sur des indices suscite toujours un certain scepticisme. Les violations des principes généraux de la protection des données sont certes difficilement concevables, mais ne sont pas invraisemblables. La proportionnalité du traitement des données surtout se révèle être une pierre d'achoppement; on ne peut l'apprécier de manière probante que lorsque l'on sait si la saisie des cas suspects peut fournir une contribution notable à la lutte contre les fraudes ou non.

Nous avons attiré l'attention du représentant des assurances que la saisie d'indices peut tout à fait constituer un traitement de données portant atteinte à la personnalité et que pour nous prononcer de manière définitive, il nous faudrait disposer d'autres éléments d'appréciation essentiels. Il est vrai que les assurances ne peuvent donner des renseignements sur ces éléments que si elles procèdent à un traitement de données basé sur des soupçons durant un certain temps. Sur ce point le dialogue entre les assurances et nous est encore en cours.

1.6.3 Obligation de garder le secret ou de renseigner des assureurs privés vis-à-vis de l'administration des impôts

Nous avons reçu une demande émanant du canton de St-Gall, nous invitant à examiner les relations entre diverses dispositions légales. La question posée était de savoir s'il était possible que l'administration cantonale des impôts reçoive des données dans le cadre de l'application de la LAVS alors qu'elle n'y avait pas droit dans le cadre de l'application de la LAA. En analysant la genèse des deux dispositions légales, nous avons constaté que cette différence a été explicitement voulue par le législateur. L'administration cantonale des impôts a par ailleurs la possibilité dans le cadre de la LAA d'atteindre ce but, en effectuant une taxation d'office et en contraignant ainsi le contribuable à fournir la preuve que cette taxation est fausse.

La question à examiner était de savoir si un assureur privé dans le domaine de l'assurance obligatoire pouvait ou devait communiquer au service des impôts des données personnelles ou s'il était soumis à l'obligation du secret en vertu de l'art. 33 de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA). Les autorités de taxation saint-galloises peuvent, en vertu de l'art. 172 al. 1 lit. c et al. 2 de la loi fiscale du canton de St-Gall (désignée ci-après par LI SG), demander à l'assureur de lui fournir des attestations concernant les prestations versées dans les cas où le contribuable ne lui a pas fourni l'attestation bien qu'il ait été mis en demeure. La première question qui se pose est de savoir si cette disposition cantonale est en mesure d'annuler l'obligation de garder le secret ancrée dans l'art. 33 LPGA et d'autoriser ainsi l'assureur à communiquer les données demandées. Selon l'art. 49 al. 1 de la Constitution fédérale, qui prévoit que le droit fédéral prime le droit cantonal qui lui est contraire, cette question ne pourrait trouver de réponse affirmative que si le législateur avait prévu dans la loi fédérale sur l'assurance-accidents (LAA) la possibilité d'autres autorisations légales pour la communication de données. Étant donné que ceci n'est pas le cas (ni la LPGA, ni la LAA ne renvoient à d'autres autorisations légales pour la communication des données), l'art. 172 al. 1 lit. c LI SG mis en relation avec l'al. 2 ne constitue pas une disposition d'exception à l'art. 33 LPGA. A notre avis, la deuxième phrase de l'art. 172 al. 2 LI SG, qui réserve le secret professionnel protégé par la loi, semble également jouer en faveur du même résultat. Vu qu'il s'agit d'une disposition cantonale, nous avons exprimé notre avis de façon réservée.

On nous a également demandé d'examiner la raison pour laquelle une obligation de garder le secret existe dans le domaine des assurances-accidents alors que dans le cadre de l'application de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS),

l'autorité fiscale peut exiger des données. Les dispositions en vigueur de l'art. 50a LAVS d'une part et de l'art. 97 LAA d'autre part, concernant la communication de données (respectivement concernant les exceptions à l'obligation de garder le secret) contiennent bien divers points communs, mais diffèrent également sur certains points. Les deux dispositions mentionnent une série de cas dans lesquels les organes des assurances sociales sont autorisés «à communiquer des données, dans des cas d'espèce et sur demande écrite et motivée (…) en dérogation à l'article 33 LPGA». Il s'agit en l'occurrence des articles 50a al. 1 lit. e LAVS et 97 al. 1 lit. i LAA. La réglementation LAA contient dans ses quatre chiffres un texte absolument identique à celui contenu dans les quatre chiffres de la lettre correspondante de la disposition de la LAVS. Ce qui frappe, c'est que la LAVS contient encore un chiffre 5 qui autorise à communiquer des données aux autorités fiscales, «lorsqu'elles leur sont nécessaires pour appliquer les lois fiscales». Ce point n'a pas de correspondance dans la LAA et l'on peut se demander s'il s'agit d'une négligence du législateur ou si cette distinction a été introduite volontairement. Nous avons examiné la question et constaté que les dispositions de la LAVS et de la LAA relatives à la communication de données ont toutes deux été récemment révisées à deux reprises, chaque fois en même temps. La dernière révision a eu lieu le 1.1.2003 dans le cadre de l'entrée en vigueur de la LPGA, alors que l'avant-dernière a eu lieu le 1.1.2001 dans le cadre de l'adaptation et de l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales aux règles de la loi fédérale sur la protection des données. Selon les déclarations faites dans le message (FF 2000 219), le but de la révision de 2001 n'était pas de modifier les dispositions. Le but poursuivi était plutôt de remplir les exigences de la loi sur la protection des données en incluant dans une loi au sens formel les autorisations de communiquer les données, qui jusqu'ici n'étaient en grande partie prévues qu'au niveau des ordonnances (ch. 1.2.2 et 1.3 du message cité). A la lecture des considérations du message, on peut admettre que les différences entre les dispositions ont délibérément été introduites par le législateur et existaient d'ailleurs déjà avant la révision au niveau des ordonnances. Ainsi, le chiffre 1.3.3. du message dit que «la liste des cas de communication a été harmonisée le plus possible dans les différentes assurances sociales». Et dans le chiffre 2.1.4, il précise que «la communication de données aux autorités fiscales (…) ne subit aucun changement de fond par rapport aux dispositions et à la pratique actuelle». La différence entre LAVS et LAA n'a pas non plus été introduite par la deuxième des révisions précitées. Ainsi, l'art. 50a al. 1 lit. e LAVS a, mis à part quelques modifications d'ordre rédactionnel et la mention de l'art. 33 LPGA, repris l'art. 50a al. 1 LAVS (les lettres a à e de cet alinéa correspondent aux nouvelles lettres 1 à 5; pour le texte exact de l'ancienne disposition, voir RO 2000 2749). En ce qui concerne la LAA, la situation est, à l'exception d'un article dont le nu-

méro a été modifié, la même: le nouvel art. 97 al. 1 lit. i correspond avec ses 4 chiffres aux lettres a à d de l'ancien article 102a al. 1 LAA (RO 2000 2760). La même déclaration – à savoir que la différence en cause n'avait pas été introduite par cette révision – découle également des chiffres 2.1.1.5 et 2.1.5.6 du message relatif à la modification de l'annexe de la LPGA, qui dit que les dispositions en vigueur jusqu'ici continueraient à rester valables (FF 2002 763).

Sur la base de ces considérations, nous sommes arrivés à la conclusion que l'assureur-accident selon LAA était obligé de garder le secret vis-à-vis de l'autorité de taxation. Cela ne doit pas pour autant signifier que l'autorité ne peut pas faire son travail parce que c'est elle qui doit prouver les faits justifiant une imposition fiscale ou une augmentation de l'impôt, car l'art. 177 LI SG prévoit la possibilité d'une imposition d'office, notamment pour les cas où le contribuable n'a pas rempli ses obligations en matière de procédure, malgré une mise en demeure. La raison d'être de la taxation d'office est justement de pouvoir fournir au contribuable, au cas où des indices sérieux existent, la preuve qu'il possède des sources de revenus qui ne sont pas indiquées dans la déclaration d'impôt.

1.6.4 Examen des faits auprès d'un service de médecin-conseil dans le domaine de l'assurance-maladie obligatoire

Au cours de l'année 2006, nous avons procédé à un examen des faits auprès du service de médecin-conseil de la société d'assurance-maladie CSS et y avons constaté des lacunes. Ceci nous a incités au printemps 2007 à adresser six recommandations à la CSS.

Au début 2006, la presse a rapporté des violations possibles de la protection des données au sein de la CSS, notamment au service de médecin-conseil. Elle a relevé en particulier qu'un nombre excessivement élevé de collaborateurs de la CSS – on parlait d'environ 400 personnes – avait accès à des données sensibles concernant des assurés. Dans le cadre de nos activités de surveillance, nous avons décidé d'établir les faits. Notre examen a révélé que le Service de médecin-conseil de la CSS présentait effectivement des lacunes au niveau de la protection des données. En raison de l'absence de procédure standardisée régissant l'octroi des autorisations d'accès, il n'est toutefois plus possible de dire rétrospectivement si des personnes non autorisées ont eu accès aux données sensibles du Service de médecin-conseil. Cette question devra être élucidée dans le cadre de la procédure pénale engagée par l'OFSP en mai 2006. La question de savoir si quelque 400 personnes ont effectivement eu accès à des données sensibles de ce service doit donc pour l'instant rester sans réponse.

Sur la base des résultats de l'établissement des faits, nous avons au printemps 2007 adressé six recommandations à l'intention de la CSS pour garantir que son service de médecin-conseil se conforme dorénavant aux prescriptions régissant la protection des données.

La première recommandation vise à mieux protéger les dossiers des patients. Ces dossiers sont, pour la plupart, encore traités et conservés sous forme papier. Les locaux où travaillaient les collaborateurs du Service de médecin-conseil n'étaient pas séparés des postes de travail des autres collaborateurs de la CSS, si bien qu'aucun contrôle d'accès systématique ne pouvait avoir lieu. Nous avons recommandé à la CSS de doter son Service de médecin-conseil des infrastructures et de locaux séparés dont il a besoin et de veiller à ce que les données dont dispose ce service soient toujours traitées de façon confidentielle vis-à-vis de l'assurance et des tiers.

La deuxième recommandation vise à renforcer l'indépendance du Service de médecin-conseil. Ce service est en effet actif non seulement dans le cadre de l'assurance de base, comme le prescrit la loi fédérale sur l'assurance-maladie (LAMal), mais aussi dans celui des assurances complémentaires au sens de la loi sur le contrat d'assurance (LCA) en tant que service d'expertise médicale. Ce double rôle présentait visiblement un conflit d'intérêts qui à notre avis n'assurait pas suffisamment l'indépendance prescrite dans le domaine de l'assurance de base. C'est pourquoi nous avons toujours jugé absolument nécessaire d'opérer une séparation stricte en termes de personnel entre le Service de médecin-conseil dans le domaine de la LAMal et le service d'expertise médicale dans le domaine de la LCA.

La troisième recommandation vise elle aussi à renforcer l'indépendance du Service de médecin-conseil. Ainsi, nous avons recommandé que le chef de ce service ne soit plus, comme jusqu'ici, subordonné au chef de la Division Prestations, mais directement à la direction générale.

Les recommandations quatre et cinq concernaient l'octroi des autorisations d'accès au système électronique de gestion des demandes auprès du Service de médecin-conseil. Dans une quatrième recommandation nous avons ainsi demandé de faire en sorte que les collaborateurs des services administratifs ne puissent avoir accès aux informations sensibles relatives aux assurés en cas de décision négative. Dans la cinquième recommandation, nous avons demandé que les devoirs et les obligations des experts médicaux qui ont accès aux données sensibles soient décrits de façon aussi détaillée que possible. De plus, le nombre de personnes disposant de tels droits d'accès étendus doit être aussi restreint que possible et réexaminé en permanence.

Enfin, dans notre sixième recommandation, nous avons demandé à la CSS de soumettre son Service de médecin-conseil à un audit externe afin de déterminer si ce dernier exerce ses activités en conformité avec la protection des données. Nous avions en effet estimé que le nombre de personnes ayant accès aux données sensibles du Service de médecin-conseil – soit environ 120 personnes selon les indications de la CSS – était trop élevé. Le nombre approprié – qui doit tenir compte des principes de proportionnalité et de finalité – doit être déterminé sur la base d'une analyse détaillée et étayée des processus internes. Dans le cadre de l'établissement des faits, la CSS n'a été en mesure de fournir des indications précises ni sur le nombre effectif des autorisations d'accès, ni sur le nombre qui serait nécessaire. Cette situation montre à notre avis à quel point il est nécessaire de procéder à un audit externe, indépendant et systématique. Nous avions à ce sujet également défendu le point de vue qu'un tel audit devrait être répété à intervalles réguliers en raison de la complexité de la matière, des changements qui peuvent intervenir et de la gravité du danger potentiel.

La CSS a accepté toutes les recommandations sans problème. Elle a, comme nous l'avions recommandé, mandaté un audit externe. Elle nous a ensuite communiqué, en joignant un rapport, que cet audit a été effectué par l'Association Suisse pour Systèmes de Qualité et de Management (SQS). Ce qui nous semble important dans ce contexte est que la CSS a décidé de se soumettre à l'avenir à intervalles réguliers à un tel audit externe. Nous saluons cette initiative de la CSS et attendons des autres institutions et entreprises qu'elles suivent ce bon exemple. A la fin de l'année, la CSS nous a communiqué qu'elle avait mis en place toutes les mesures contenues dans nos recommandations.

L'examen des faits auprès de la CSS représente un tournant dans notre collaboration avec l'OFSP. Ainsi, l'enquête actuellement en cours sur l'organisation en matière de protection des données du service de médecin-conseil des assureurs-maladie a pour but d'adopter une attitude commune en ce qui concerne les questions de protection des données (cf. également le ch. 1.6.5).

1.6.5 Enquête sur l'organisation en matière de protection des données du Service de médecin-conseil des assureurs-maladie

En collaboration avec l'OFSP, nous procédons depuis décembre 2007 à une enquête sur l'organisation en matière de protection des données auprès de tous les assureurs-maladie. Cette action a notamment pour but de soutenir les organes de surveillance pour qu'ils élaborent des critères pour une structure d'organisation qui soit conforme aux exigences de la protection des données.

Ces dernières années, des reproches ont été formulés à plusieurs reprises concernant des traitements abusifs de données personnelles par les assureurs-maladie. Ces reproches ont eu pour suite une enquête de la part de l'OFSP – autorité de surveillance – et du PFPDT, ainsi que des interventions parlementaires. Ainsi, des examens ont été faits auprès de certains assureurs-maladie, aussi bien par l'OFSP que par nous-mêmes. Ceux-ci ont révélé qu'il y avait bel et bien des lacunes qui rendaient possibles des utilisations abusives de données personnelles. En réponse à une initiative parlementaire, le Conseil fédéral a mandaté l'OFSP de soumettre à l'avenir plus fréquemment les fichiers des assureurs à un contrôle et d'impliquer également le PFPDT dans cette tâche. Divers assureurs-maladie ont d'ailleurs émis d'eux-mêmes le souhait que les deux organes de surveillance collaborent plus étroitement. C'est la raison pour laquelle nous faisons actuellement, en collaboration avec l'OFSP, une enquête auprès de tous les assureurs-maladie sociaux reconnus. Un questionnaire détaillé sur l'organisation et sur la protection des données, élaboré avec l'aide du PFPDT, a été envoyé à tous les assureurs. Ils ont été invités à le remplir jusqu'au 15 février 2008 et à fournir les documents à l'appui de leurs réponses.

L'objectif important de ce sondage est d'appuyer les organes de surveillance dans l'élaboration de critères pour une structure d'organisation des assureurs qui soit conforme aux exigences de la protection des données. Il doit en outre également permettre d'optimiser les processus de contrôle des prestations du point de vue de la protection des données. Il est prévu de mettre au point ces critères sous forme de recommandations en automne 2008. Ces critères doivent aider les assureurs-maladie à assumer leur responsabilité afin de respecter les exigences de la protection des données.

1.6.6 Preuve d'identité lors de demandes de renseignement pour le pool de données de santésuisse

Nous avons, à la demande de santésuisse, examiné sous l'angle de la protection des données le processus de fourniture de renseignements dans le cadre de leur pool de données. Bien que santésuisse ait pris en compte toutes nos remarques, la procédure de vérification de l'identité a été modifiée peu après suite à l'intervention d'un médecin concerné.

Santésuisse traite sous le nom «pool de données» une grande quantité de données provenant des assureurs-maladie, notamment dans le but de pouvoir évaluer le caractère économique des activités des fournisseurs de prestations, en l'occurrence des médecins. Au début de juillet 2007, cette institution nous a demandé de donner notre appréciation sur la démarche adoptée lors de la fourniture de renseignements au sens de l'art. 8 LPD. La fourniture de renseignements en cause concerne un fichier qui résulte de l'application de la loi fédérale sur l'assurance-maladie (LAMal). Cela signifie donc que ce traitement nécessite en fait une base légale. Il faut relever que les dispositions de la LAMal relatives au contrôle de rentabilité ont été formulées de manière plutôt vague, laissant une large liberté d'interprétation. Il nous a semblé important de souligner que le PFPDT s'occupe dans son activité en premier lieu des questions de protection des données liées aux informations qui concernent les patients. En ce qui concerne les questions relatives aux données des prestataires de service, le PFPDT part du principe que celles-ci devraient en premier lieu être jugées par les partenaires tarifaires ou, éventuellement, par l'OFSP. Dans le cas présent, nous avons pu constater sur la base des informations qui nous ont été fournies que les données traitées n'avaient pas de relation avec des patients.

Par rapport au contenu du renseignement, nous avons tout d'abord constaté que la formule utilisée dans la loi «toutes les données concernant la personne concernée qui sont contenues dans le fichier» (cf. art. 8 al. 2 lit. a LPD) implique notamment deux choses: tout d'abord, il convient de communiquer à la personne concernée non seulement les données brutes, mais également les données dérivées de ces dernières. Deuxièmement, ces données doivent être communiquées à la personne concernée indépendamment de leur mode physique de stockage (électronique ou sous forme papier) chez le maître de fichier. Nous avons cependant jugé raisonnable que les médecins concernés ne reçoivent pas de copie de leur correspondance avec santésuisse concernant la fourniture de renseignement dans le cadre du pool de données. On peut en effet admettre que les documents en question se trouvent déjà auprès des

médecins concernés. Il peut néanmoins être nécessaire, en fonction de la manière dont la demande de renseignement est formulée, de mentionner explicitement cette restriction, conformément au principe de bonne foi.

En ce qui concerne le contrôle de l'identité du médecin requérant, nous avions d'abord conseillé à santésuisse d'appliquer la procédure standard telle que décrite dans le message relatif à la LPD, dans différents documents publiés par le PFPDT ainsi que dans les deux éditions du commentaire, à savoir que pour se légitimer la personne concernée joint à sa demande de renseignement écrite la copie d'une pièce d'identité. Un médecin concerné s'est alors adressé à nous et s'est plaint de cette exigence, en fournissant plusieurs justifications. En bref, il a argumenté qu'une telle vérification d'identité n'est premièrement pas nécessaire puisque santésuisse possède déjà toutes les informations telles que l'adresse, l'autorisation de cabinet, le numéro de concordat et le numéro EAN. Quant au passeport, il ne contient, mis à part le nom et la date de naissance, aucune indication qui pourrait être utile pour le contrôle d'identité effectué par santésuisse. Deuxièmement, des indications fournies sur une copie seraient très simples à falsifier, ce qui signifie que le fait de joindre une copie n'offre aucune sécurité supplémentaire. Troisièmement, le passeport contient des informations sur le physique de la personne que le destinataire n'a pas besoin de connaître. Quatrièmement, la remise sûre au bon destinataire dépend uniquement de l'adresse correcte sur l'envoi. Les arguments fournis nous paraissant convaincants, nous avons contacté santésuisse qui s'est tout de suite déclaré prête à adapter sa procédure de fourniture de renseignement. La nouvelle procédure modifiée ne nécessite en règle générale plus de contrôle d'identité, puisque la personne qui demande le renseignement est connue de santésuisse. Ce n'est que dans les cas où un doute existe sur l'adresse à laquelle le renseignement doit être envoyé qu'il sera opportun de procéder à une vérification de l'identité du médecin requérant.

1.7 Secteur du travail

1.7.1 Surveillance vidéo à la poste

La Poste est confrontée au phénomène des délits commis par des employés de l'entreprise. Un système de surveillance par vidéo devrait lui permettre de lutter contre ces pratiques. Grâce à la mise en œuvre de techniques modernes de cryptage et à un décryptage restrictif des enregistrements, le problème de l'interdiction de la surveillance du comportement sur le lieu de travail est pour une grande partie résolu.

En 1999 déjà, la surveillance par vidéo à la Poste a fait l'objet d'une de nos interventions (cf. notre 7ème rapport d'activités 1999/2000, ch. 6.1). Nous étions alors arrivés à la conclusion que la surveillance par vidéo n'était pas conforme au droit car elle violait l'interdiction de surveillance du comportement. En 2007, la Poste a mis au point un nouveau projet de surveillance par vidéo et nous a priés de l'examiner sous l'angle de la protection des données.

Des délits commis par des employés de l'entreprise sont à l'origine du nouveau projet de surveillance par vidéo. La Poste et sa clientèle subissent un préjudice majeur du fait de ces délits. A la demande de l'entreprise, les centres de tri de la Poste seront à l'avenir surveillés de manière systématique par des caméras vidéo. De l'avis de la Poste, la plupart des mesures de sécurité actuelles ont uniquement un caractère de prévention et ne couvrent qu'insuffisamment les besoins de sécurité des centres de tri postal. Selon les renseignements fournis par l'entreprise, les mesures actuellement en cours sont notamment les audits de sécurité, les contrôles sporadiques des personnes et de leurs effets ainsi que des canaux spéciaux protégés pour les clients particuliers qui, d'expérience, sont régulièrement victimes de vols. En outre, des mécanismes de distribution automatique du courrier ainsi que la technologie RFID pour le traçage de certains envois seront mis en œuvre à l'avenir.

La Poste justifie son nouveau projet de surveillance par vidéo essentiellement en invoquant une meilleure prévention et une méthode plus efficace devant confondre les auteurs d'infractions et de disculper les non coupables. Dans le secteur du tri manuel, il est prévu que certains employés soient dans le champ des caméras de surveillance durant toute leur journée de travail. Il existe néanmoins une rotation hebdomadaire à des endroits non surveillés. Une surveillance permanente (monitoring des images en direct) n'est pas prévue. L'entreprise justifie la durée de conservation de 100 jours des

vidéos par la possibilité de procéder efficacement aux recherches des pertes annoncées avec retard (par ex. en relation avec des envois internationaux). Le personnel est informé comme il se doit des mesures de sécurité actuelles et des mesures prévues. L'entreprise a confirmé que les associations de personnel ont été consultées.

Après avoir examiné le projet, nous avons d'abord exposé à la Poste ce que recouvre la protection du comportement en tant qu'aspect de la notion de personnalité. A ce propos, nous avons souligné en particulier que le sentiment négatif d'être constamment sous surveillance est à même de provoquer une pression psychologique telle qu'avec le temps, elle pourrait provoquer des problèmes de santé.

Nous avons ensuite expliqué que les surveillances par vidéo à titre d'administration et de conservation de la preuve sont du ressort exclusif des autorités pénales en raison de la gravité de l'atteinte à la personnalité. La responsabilité de mettre en place une surveillance par vidéo relève donc des autorités publiques, du fait que l'on admet que celles-ci sont en mesure de prendre des décisions neutres et conformes au droit. L'interdiction de surveillance du comportement n'admet donc pas une surveillance systématique par l'employeur. Ce n'est que dans un état de nécessité grave que l'employeur peut lui-même mettre en place un tel système et surveiller le comportement des employés.

Nous avons également souligné que cette situation juridique comporte des difficultés pratiques. En effet, les autorités compétentes ne sont guère en état de répondre au besoin général des particuliers de sauvegarder des preuves par surveillance vidéo. L'expérience montre que les demandes de surveillance adressées aux autorités compétentes sont souvent laissées aux bons soins du requérant. Nous avons toutefois assuré à la Poste que la technologie actuelle permet de remédier à cette difficulté pratique. Nous avons expliqué que les surveillances systématiques par vidéo peuvent désormais être considérées comme conformes à la loi si les données enregistrées sont cryptées. Le cryptage systématique des images et la limitation du décryptage à des cas de soupçon concret réduisent en effet à un minimum le sentiment de surveillance systématique du comportement. Cette conclusion nous a été inspirée essentiellement par le rapprochement entre la surveillance par vidéo et la surveillance de l'utilisation d'Internet et du courrier électronique par l'employeur où les surveillances du comportement systématiques, mais pseudonymisées peuvent, à certaines conditions, être considérées comme licites.

Nous avons en outre recommandé à la Poste de restreindre l'accès aux enregistrements et leur décryptage par un système de double cryptage: l'entreprise possède la première clé d'accès et un tiers (par ex. un délégué du personnel) la seconde. Cette solution permet de limiter le décryptage des enregistrements à des cas de soupçon

concret, en respectant le principe «des quatre yeux». Enfin, l'information préalable des personnes concernées sur le cryptage et le décryptage restrictif est effectuée de manière centrale.

Nous avons finalement informé la Poste que l'implantation de telles solutions techniques permet de résoudre dans une large mesure le problème de l'interdiction de la surveillance du comportement par la surveillance par vidéo à la place de travail (voir à ce sujet ch. 1.2.3).

1.7.2 Le traitement des données techniques liées aux communications téléphoniques par l'Office fédéral de l'informatique et de la télécommunication

Le traitement, en particulier la transmission de données techniques accessoires liées aux communications téléphoniques entre l'administration fédérale et certaines autorités d'enquête et unités finales d'imputation des coûts, par l'Office fédéral de l'informatique et de la télécommunication (OFIT), nécessite des bases légales. En vue de leur création la Confédération a constitué un groupe de travail ad hoc. En attendant l'élaboration et l'entrée en vigueur de ces bases légales, nous avons recommandé à l'OFIT de s'en tenir à notre solution transitoire. Ainsi, la transmission des données techniques concernant des appels privés vers les unités finales d'imputation des coûts se limite à l'indicatif des numéros composés. Quant aux autorités d'enquête, les données techniques liées aux communications téléphoniques ne peuvent leur être communiquées qu'en cas d'indices fondés.

L'OFIT sert de trait d'union entre le fournisseur de services de télécommunication Swisscom et les organes de la Confédération. A ce titre, l'office fédéral transmet régulièrement un certain nombre de données techniques accessoires concernant les communications téléphoniques aux unités finales d'imputation et, sur demande, aux autorités d'enquête de la Confédération. Du fait de l'absence de réglementation légale, l'OFIT est souvent confronté à la question de son droit de communiquer des données, surtout lorsque les demandes émanent d'autorités d'enquêtes désireuses de consulter ces données. L'office nous a donc demandé de déterminer les conditions dans lesquelles un traitement de données serait conforme à la protection des données. Après avoir examiné la question sous différents angles, nous avons opéré une distinction entre la communication régulière de données aux services financiers et la communication aux autorités d'enquête dans un cas d'espèce.

Nous avons retenu que la communication régulière des données aux unités de la Confédération en charge de l'imputation finale des coûts nécessite des bases légales; or ces bases n'existent pas. Dans ce contexte, un groupe de travail interdépartemental chargé de combler cette lacune a été créé sous la direction de l'Office fédéral de la justice. L'OFIT et nous-mêmes participons à ce groupe de travail.

Conformément à la législation sur les télécommunications, le cocontractant peut exiger du fournisseur de services de télécommunication qu'il lui communique, lors de la facturation, l'ensemble des données concernant les appels téléphoniques. Toutefois, nous estimons qu'il n'est pas nécessaire, pour la facturation, de donner l'ensemble du numéro composé à titre privé. Nous avons donc recommandé à l'OFIT de restreindre au seul indicatif les données relatives aux appels téléphoniques privés effectués chez Swisscom.

S'il s'agit d'appels sur le réseau de téléphonie fixe, la personne peut différencier les appels privés des appels professionnels en appuyant sur une touche avant d'entamer la communication. Cela nécessite néanmoins une centrale téléphonique possédant les moyens techniques appropriés. Tel est le cas à la Confédération. En ce qui concerne le réseau de téléphonie mobile, la manière la plus simple de différencier les données des appels privés et des appels professionnels est d'utiliser deux cartes SIM.

Nous avons également constaté que la communication de données téléphoniques accessoires aux autorités menant des enquêtes pénales ou administratives au niveau fédéral interne ne reposait pas sur une base légale. Nous avons donc recommandé à l'OFIT de ne pas communiquer systématiquement ces données aux autorités d'enquête à chacune de leurs demandes, mais uniquement en présence d'indices concrets et fondés au niveau de l'enquête. Des affirmations non fondées, de vagues sentiments, des impressions personnelles, des suppositions ou le simple manque de confiance envers un employé ne constituent généralement pas une base suffisante pour justifier l'ouverture d'une enquête et, partant, pour que l'OFIT communique des données accessoires aux autorités d'enquête.

1.7.3 Recommandation concernant les tests de dépistage de la consommation de drogues et d'alcool effectués par les CFF

Au printemps 2007, la presse a fait état des tests de dépistage de la consommation de drogues effectués par les CFF. Il s'agissait, pour les CFF, de contrôler les employés de moins de 40 ans exerçant des tâches liées à la sécurité pour vérifier s'ils prenaient des drogues illégales. En cas de résultat positif, les personnes concernées devaient s'engager par écrit à ne plus consommer de cannabis, même pendant leur temps libre. Nous avons notamment recommandé aux CFF de fixer des valeurs limites pour les tests de dépistage de la consommation d'alcool et de drogues au-dessous desquelles aucun traitement de données ne doit être effectué.

Nous avons tout d'abord constaté qu'il n'existe actuellement aucune base légale suffisante permettant de procéder à des tests de dépistage de consommation de drogues. Ni les dispositions en vigueur, ni les dispositions prévues dans la réforme des chemins de fer 2 ne prévoient des analyses d'urine, des analyses de sang ou d'autres analyses invasives en l'absence d'indication thérapeutique. Les futures dispositions de la réforme des chemins de fer 2 prévoient par contre la possibilité de procéder inopinément et sans soupçons concrets à des alcootests. La pratique actuelle montre cependant que certains collaborateurs sont obligés de se soumettre à des tests de dépistage de consommation de drogues, même en l'absence de tout soupçon.

Forts des résultats de nos éclaircissements, nous avons recommandé aux CFF, pour procéder à des tests de dépistage, de se fonder sur les dispositions correspondantes du projet de loi relatif à la réforme des chemins de fer 2. Nous leur également recommandé de fixer des valeurs limites pour les tests de consommation d'alcool et de drogues. Le non dépassement de ces valeurs ne doit donner lieu à aucun traitement de données.

Suite à cette recommandation, l'Office fédéral des transports (OFT) s'est déclaré prêt, pour la période allant jusqu'à l'entrée en vigueur de la base légale, à examiner et à introduire des valeurs limites sur la base d'une directive.

La recommandation se trouve à l'annexe 4.4 du présent rapport d'activités.

1.7.4 Révision de la loi sur le personnel de la Confédération

La loi sur le personnel de la Confédération fait actuellement l'objet d'une révision complète. Cette révision permettra notamment de définir dans la loi les nouvelles tâches du système d'information sur le personnel de la Confédération (BV PLUS). Parmi ces tâches figurent notamment l'évaluation des collaborateurs ainsi que la saisie du temps de travail. La procédure d'appel (E-Gate) et les nouveaux services bénéficiant d'une autorisation d'accès doivent également être prévus dans la nouvelle loi.

Dans le cadre de la consultation des offices relative à la révision de la loi sur le personnel de la Confédération (LPers), nous avons constaté que l'élargissement du système de traitement des données BV PLUS à de nouvelles tâches (dont certaines sont déjà prises en compte et d'autres sont encore à prendre en compte par le législateur) ne pouvait plus être ignoré. Nous avons en particulier demandé que les évaluations des collaborateurs, les objectifs convenus et la saisie du temps de travail doivent être intégrées explicitement dans le nouveau texte de loi en tant que nouvelles fonctions de BV PLUS. En outre, nous avons demandé que les accès aux données personnelles sensibles et aux profils de la personnalité soient limités aux collaborateurs concernés et à leurs supérieurs hiérarchiques et que ces accès soient fixés dans la loi. Le droit d'accès des services du personnel doit se limiter à l'évaluation et, éventuellement, à des données administratives.

En ce qui concerne la procédure d'appel (E-Gate), nous avons requis une densité normative plus élevée ainsi que, sur le plan technique, un cryptage des données. Enfin, nous avons demandé que les droits d'accès de l'Office fédéral du personnel et des services de support technique aux données saisies dans BV Plus soient régis de manière restrictive et explicite.

1.7.5 Système de gestion des données relatives au personnel de l'administration fédérale BV PLUS

Nous examinons actuellement si le système de gestion des données relatives au personnel de l'administration fédérale BV PLUS est mis en œuvre dans le respect des principes de la protection des données. Ce contrôle a pour but de comparer la situation de fait, sous l'angle technique et organisationnel, avec les bases légales en vigueur.

Nous limitons notre contrôle au respect des contraintes essentielles en matière de protection des données et ne pratiquerons des examens détaillés que par sondage. Notre contrôle porte essentiellement sur le caractère légal de la collecte des données et le respect du principe de la bonne foi, sur la conformité au but indiqué et la proportionnalité des données répertoriées, sur les mesures de sécurité concernant les données ainsi que sur la garantie des droits des personnes concernées. Dans le cadre des différents processus de BV PLUS, nos contrôles se sont portés sur plusieurs interlocuteurs. Il s'agit du Centre de compétences en matière de ressources humaines de l'Office fédéral du personnel (OFPER), du Centre de compétences SAP de l'Office fédéral de l'informatique et de la technologie (OFIT) ainsi que du Service du personnel de la Chancellerie fédérale. A titre d'exemple pour toute l'administration fédérale, le Service du personnel de la Chancellerie fédérale est contrôlé comme utilisateur final. Les éventuelles recommandations qui seront adressées à ce service sur la base des résultats du contrôle pourront, selon les circonstances, valoir pour l'ensemble de l'administration fédérale. Les contrôles effectués auprès du Service du personnel de la Chancellerie fédérale porteront essentiellement sur l'identification et l'authentification, la gestion des mots de passe, les écrans de veille et la formation; auprès du Centre de compétence SAP de l'OFIT, le contrôle est axé sur les mesures de sécurité relatives aux données et, auprès du Centre de compétence en matière de ressources humaines de l'OFPER, sur les données répertoriées.

Après avoir reçu les réponses à nos questionnaires et mené les premiers entretiens, nous avons rédigé les procès-verbaux de séance et les avons soumis aux participants pour vérification et éventuellement complément. Les réactions ne nous sont pas encore parvenues. Si nécessaire, d'autres entretiens, questions écrites ou inspections locales suivront.

1.8 Economie et commerce

1.8.1 Révision du droit de la société anonyme; usage des inscriptions au registre du commerce

Le nouveau droit de la société anonyme simplifie la communication entre la société et ses actionnaires grâce à l'utilisation des médias électroniques. Dans ce cadre, la transparence et l'actualité du registre du commerce est en outre améliorée par la fixation de délais impératifs pour l'inscription au journal. Nous sommes toutefois d'avis qu'il faut aussi établir des délais de blocage de l'accès public aux inscriptions au registre du commerce lorsque celles-ci ont perdu de leur pertinence dans les relations d'affaires. Notamment en cas de radiation (par ex. après une faillite), l'intérêt personnel à continuer à vivre sans se voir attacher des étiquettes définitives prime au bout d'un certain temps (droit à l'oubli). Pour cette raison, nous estimons inconcevable que toutes les inscriptions au registre du commerce soient accessibles librement et «ad eternam».

Le nouveau droit de la société anonyme reconnaît les potentialités de la communication électronique et prévoit pour la première fois l'usage des médias électroniques dans la communication entre la direction d'entreprise et les actionnaires. Il réglemente les possibilités d'assemblée générale (AG) «multi-sites» (les interventions images et sons sont retransmises en direct sur tous les sites), la convocation électronique de l'AG, la procuration électronique, l'utilisation des médias électroniques durant l'AG et la tenue d'une assemblée générale exclusivement électronique, pouvant renoncer entièrement à l'assemblée conventionnelle dans un lieu de réunion réel. Nous relevons à cet égard que la mise en place concrète des nouvelles formes de communication par les entreprises doit se faire dans le respect d'aspects particulièrement importants en matière de protection des données.

Au cours de cette révision, plusieurs articles ont été modifiés concernant les délais de publication dans le journal auprès du registre du commerce. Nous sommes d'avis qu'il faut aussi définir des délais pour que certaines inscriptions au registre du commerce ne soient plus accessibles d'une manière générale et publique, autrement dit qu'elles soient supprimées du registre. En effet, certaines informations publiées dans le registre du commerce perdent de leur pertinence au-delà d'un certain laps de temps et, à notre avis, elles ne devraient alors plus être accessibles au public. Cela vaut particulièrement pour les radiations (tant des procurations que des entreprises) car avec le

temps, elles ne sont plus pertinentes pour un bon déroulement des affaires. En outre, l'intérêt personnel d'une personne concernée par une radiation à pouvoir mener un vie libre d'étiquettes, en d'autres termes qui ne soit pas excessivement marquée par le passé, augmente avec le temps (droit à l'oubli). Pour cette raison, nous ne concevons pas que toutes les inscriptions au registre du commerce soient accessibles librement et «ad eternam» (cf. égal. ch. 1.8.2)

Nous avons donc proposé d'introduire aussi des délais pour le blocage de l'accès public, et cela sous forme de norme au «Titre trente: Le registre du commerce» du code des obligations. Cette modification n'étant, pour des raisons de délai, plus possible pour cette procédure de révision, nous soumettrons à nouveau notre proposition à l'occasion d'une procédure législative.

1.8.2 Publication privée de données extraites des registres du commerce

Quiconque entend participer à la vie économique en tant qu'entreprise individuelle, société de personnes ou personne morale doit être inscrit au registre du commerce. Il lui faut alors indiquer le nom complet des organes représentatifs. Ces données sont publiées dans leur totalité sur Internet, d'où elles sont reprises intégralement par des sociétés privées de renseignements commerciaux. Ces sociétés ajoutent d'autres informations à ces données, en modifient la structure et publient le résultat de leur travail également sur Internet. Cela n'est pas seulement problématique parce qu'à un moment donné, ces renseignements ne sont plus actuels. Il ne faut pas non plus que les agences de renseignements économiques aillent au-delà du traitement des données effectué par un organisme étatique.

Les sites web des sociétés de renseignements commerciaux sont très consultés. Ce succès se traduit souvent par le fait qu'une recherche sur Internet à partir du nom de personnes physiques met en évidence l'offre Internet des sociétés de renseignements. Ceci n'est pas du goût de bon nombre de personnes qui critiquent soit le fait que l'on donne des renseignements sur des éléments qui ne sont plus du tout actuels, soit le principe même que des entreprises privées reproduisent des données figurant dans les registres du commerce. Dans les deux cas, on peut invoquer un droit d'effacement à l'égard des sociétés de renseignements commerciaux. Diverses sociétés de renseignements commerciaux n'acceptent toutefois pas de se conformer à ce droit.

La plupart des réclamations qui nous sont parvenues concernaient une société en particulier. Nous lui avons donc adressé une recommandation dont la requête essentielle était de respecter à l'avenir le droit d'effacement des personnes concernées. Par ailleurs, nous avons souligné que le traitement de données devait aussi être modifié sur divers autres points: dans certaines situations, il peut y avoir une obligation à effacer les données compte tenu de leur actualité, ceci même sans demande expresse d'effacement.

La société de renseignements commerciaux a rejeté notre recommandation sur tous ses points. Nous avons donc soumis le cas pour examen au Tribunal administratif fédéral qui, depuis la révision de l'organisation judiciaire, est compétent pour traiter les actions du PFPDT.

Dans son arrêt du 26 février 2008, le Tribunal administratif fédéral a rejeté l'action du PFPDT, tout en clarifiant de nombreux points qui contribuent à la sécurité du droit pour les personnes concernées. Globalement, le Tribunal administratif fédéral parvient à la conclusion que l'intérêt de la diffusion publique d'informations du registre du commerce subsiste sans limitation temporelle indépendamment du fait que la source de données soit publique ou privée, aussi longtemps que les données ne sont pas modifiées quant au fond. Le PFPDT en prend acte, mais reste de l'avis que des données du registre du commerce qui n'ont plus d'utilité juridique et factuelle ne devraient plus être accessibles sur Internet, et que dans ce cas, l'intérêt de la personne concernée doit prévaloir sur l'intérêt d'une diffusion publique des données du registre du commerce.

Pour cette raison, le PFPDT continuera de se préoccuper du problème et proposera, le cas échéant, de créer les conditions qui, par le biais d'une révision de la législation, interdiront la diffusion de données du registre du commerce pour lesquelles il n'existe plus d'intérêt à une diffusion publique. Dans ces circonstances, le PFPDT renonce à recourir auprès du Tribunal fédéral.

1.8.3 Le traitement des données sur la solvabilité en regard de la loi sur la protection des données

Les données sur la solvabilité sont toutes les données personnelles qui fournissent des informations sur la capacité d'une personne à respecter ses engagements financiers. Elles sont traitées par de nombreux acteurs. Parmi ceux-ci figurent essentiellement les créanciers dont les factures n'ont pas été payées (ou l'ont été avec retard), les sociétés de recouvrement des créances, ainsi que les sociétés de renseignements économiques qui cherchent à prévenir le risque de défaillance de crédit grâce à des banques de données centrales. On constate dans la pratique que des incertitudes juridiques accompagnent toutes ces opérations de traitement de données. Dans le but d'améliorer la sécurité du droit, nous avons entamé un dialogue constructif avec les différents prestataires traitant les données de solvabilité.

Une grande partie de la population ignore totalement l'existence des banques de données sur la solvabilité. Si tant est que l'on aborde publiquement le sujet des banques de données des sociétés de renseignements économiques, on préfère les appeler «banques de données de débiteurs» et en tant que telles, elles débouchent parfois sur des scandales. A cet égard, il est certes vrai que des données de solvabilité fausses peuvent causer des préjudices; mais les banques de données de solvabilité remplissent aussi une fonction importante au service des acteurs de l'économie qui accordent des crédits. Il faut se garder de tirer des conclusions hâtives. En premier lieu, il convient donc d'analyser de près le problème de la chaîne du traitement des données qui implique plusieurs protagonistes, responsables en vertu du droit de la protection des données. L'accent doit être mis sur les interférences entre ces personnes.

Le premier point d'interférence est la collaboration entre créanciers et sociétés de recouvrement. Ces deux protagonistes doivent contribuer à l'examen, dans les plus brefs délais, des contestations de créance (qui portent sur l'existence de la créance ou sur son montant). Eu égard à de possibles erreurs, de nature administrative ou juridique, au niveau des prestations de la part des créanciers, on ne peut laisser simplement l'examen d'affaires contentieuses aux offices des poursuites et aux tribunaux, car cela se fait régulièrement au détriment des personnes concernées. Les créanciers et les sociétés de recouvrement doivent donc garantir qu'un traitement rapide des cas problématiques est possible (principe de l'exactitude des données). Par ailleurs, il convient de réglementer le mode d'action face à des créances qui se trouvent «dans l'incertitude» (dans l'idéal, suspension provisoire des mesures d'encaissement).

Il existe un autre point d'interférence important entre les bureaux d'encaissement et les sociétés de renseignements économiques. A cet égard, on suppose parfois à tort que le transfert de données peut se faire sans restriction. De notre point de vue, il est indispensable de définir exactement les cas dans lesquels les données peuvent être transmises et quelles sont les données qui ne peuvent l'être (principe de la proportionnalité du traitement des données). Le dialogue avec les partenaires de la branche est en cours.

Ce dernier point est également applicable à toutes les questions qui ne concernent que les sociétés de renseignements économiques. Il convient ici d'examiner notamment combien de temps un fait négatif touchant à la solvabilité (par ex. une poursuite) peut avoir des effets, quand le scoring de crédit constitue un profil de la personnalité et quelles sont les obligations auxquelles les sociétés de renseignements économiques doivent se soumettre eu égard à la transparence du traitement des données (qui laisse actuellement à désirer) (cf. aussi ch. 1.2.6).

1.9 Finances

1.9.1 Protection des données dans le trafic international des paiements (SWIFT)

Selon un article du «New York Times» daté du 23 juin 2006, la Society for Worldwide Interbank Financial Telecommunication (SWIFT) a permis aux Etats-Unis d'accéder aux données rassemblées dans le centre opérationnel sis sur territoire américain, cela dans le cadre de la lutte contre le terrorisme. Nous avons abordé les problèmes de protection des données qui se sont posés dans ce contexte avec l'appui du Conseil fédéral et des banques suisses: dans le cadre d'une solution politique avec les Etats-Unis, des garanties de sécurité ont été convenues et la clientèle des banques a été activement informée de la possible transmission de données aux autorités américaines. La SWIFT a en outre annoncé qu'à l'avenir elle ne traiterait plus aux Etats-Unis que les données des transactions concernant le trafic des paiements transatlantique. Afin de pouvoir concrétiser cette solution du point de vue technique, la SWIFT a décidé de créer en Suisse un troisième centre opérationnel.

Suite aux révélations faites par le «New York Times» selon lesquelles les autorités américaines de lutte contre le terrorisme ont accès aux données des transactions bancaires du réseau SWIFT (cf. notre 14ème rapport d'activités 2006/2007, ch. 1.8.1), des mesures initiées par nous-mêmes et par le gouvernement suisse ont été prises pour que la protection des données dans le trafic international des paiements soit respectée. Après avoir analysé les faits, nous sommes parvenus à la conclusion que la transmission de données des transactions bancaires par la SWIFT avait violé la LPD à deux égards. D'une part, les instituts financiers sis en Suisse n'ont pas accompli leur devoir d'information à l'égard de leurs clients; en effet, ils ont omis de les aviser de la communication de données par la SWIFT respectivement de la possibilité d'une telle communication. D'autre part, il y a eu un transfert de données aux Etats-Unis, qui n'a pas un niveau de protection des données adéquat. Les deux problèmes ont été résolus en coopération avec le gouvernement suisse et avec les instituts financiers sis en Suisse.

En ce qui concerne le devoir d'information des banques, nous avons emprunté le chemin novateur d'une «autorégulation surveillée» des banques en ce sens que nous avons laissé aux banques le soin de s'acquitter de leur devoir d'information d'une

manière qui corresponde au mieux à leurs besoins. Nous avons choisi ce chemin essentiellement compte tenu de la confiance dont bénéficie la place financière suisse. En étroite collaboration avec l'Association suisse des banquiers, nous avons rédigé une lettre d'information aux clients des banques grâce à laquelle il a été satisfait au devoir d'information. Cette lettre a déjà été envoyée par les banques suisses. En comparaison avec les pays étrangers européens où ce genre d'information se fait par une simple mention dans les CG (Conditions générales), nous avons ainsi obtenu une information active des clients suisses par les banques. En même temps, l'information active et autonome de la clientèle par les banques a renforcé la confiance en une protection des données efficace.

Il était nécessaire de parvenir à une solution politique qui respecte à la fois les objectifs de la lutte contre le terrorisme et le régime de protection des données des pays concernés (y compris la Suisse). Une solution satisfaisante a donc été négociée. A cet effet, des garanties de sécurité lors de l'accès aux données du réseau SWIFT ont été convenues avec les Etats-Unis. Ainsi, les autorités américaines ne peuvent demander à la SWIFT d'entamer une demande de recherche dans ses données que s'il est prouvé qu'une personne cible a un lien avec le terrorisme ou son financement. Les résultats de la recherche ne sont communiqués aux autorités américaines que si la recherche a été positive. Par ce moyen, les autorités américaines ont accès aux données en question uniquement s'il s'agit d'analyser un état de fait concret et déjà existant. En outre, toutes les recherches, y compris les preuves qui ont mené à la recherche, sont consignées. Par ailleurs, la convention prévoit qu'une personnalité européenne connue sera nommée et aura pour tâche de vérifier que le programme est appliqué conformément aux engagements pris à l'égard du contrôle de la protection des données personnelles provenant de l'Union européenne. Les autorités américaines garantissent ainsi, en ce qui concerne les données SWIFT, une protection des données conforme au droit suisse.

Dans le cadre de la réorganisation de l'entreprise commerciale et étant donné la forte augmentation du volume des transferts au cours des dernières années, la SWIFT a décidé de créer d'ici fin 2009 un troisième centre opérationnel en Suisse, en plus des deux centres existant déjà en Belgique et aux Etats-Unis et, ce faisant, de séparer le trafic des transactions en deux zones (une zone européenne et une zone transatlantique). Dans ce cadre, les virements intra-européens seraient traités par les deux centres opérationnels situés en Suisse et en Belgique et les virements transatlantiques par les centres opérationnels américain et suisse. Etant donné que les autorités américaines n'ont accès qu'aux données qui sont traitées dans le centre opérationnel américain, les autorités américaines n'auront à l'avenir plus directement accès à tous les virements intra-européens.

1.9.2 Communication de données du trafic international des paiements à des gouvernements étrangers, dans la perspective de l'application de sanctions

Dans le cadre de leurs activités internationales, les instituts suisses de crédit peuvent avoir besoin de prouver à des Etats étrangers (notamment les Etats-Unis) qu'elles respectent les sanctions requises par ces derniers. Faute de quoi l'accès commercial à l'Etat demandeur pourrait, selon les cas, être entravé. Dans ce contexte, un institut suisse de crédit a envisagé, dans le cadre du trafic international des paiements dans lequel il officie au titre de banque de transfert, de communiquer volontairement des données de transfert aux Etats-Unis. Après avoir examiné les faits et la situation juridique, nous avons conclu que pour prouver le respect des sanctions, seule une transmission volontaire de données de transferts anonymisées était autorisée.

Nous avons examiné, pour un institut suisse de crédit, la question de savoir dans quelle mesure la LPD autorisait la transmission de données à des autorités étrangères dans le cadre d'opérations de transferts internationaux. Dans le cas concret, l'institut suisse était un maillon dans la chaîne des flux de paiements internationaux et voulait apporter la preuve aux autorités américaines qu'il avait respecté les sanctions américaines contre l'Iran dans le cadre d'opérations de transfert.

La LPD s'applique du fait que les transferts nécessitent un traitement de données personnelles. La communication de données n'est donc possible que s'il n'y a pas atteinte illicite à la personnalité de la personne concernée. Vu que la transmission de données aux autorités américaines ne repose sur aucune base légale et qu'un intérêt prépondérant public ou privé n'est pas manifeste, nous avons examiné dans quelle mesure on pouvait supposer l'existence d'un consentement implicite.

L'institut suisse de crédit a avancé à cet égard l'argument selon lequel la personne qui fait exécuter un mandat de transfert en dollars américains doit s'attendre à ce que le traitement des données se fasse aux Etats-Unis. Dans le monde de la finance nul n'ignore que les transactions sur devises, à de rares exceptions, ont lieu dans le pays de la monnaie correspondante et que de ce fait, les banques intérieures entretiennent avec les banques étrangères des relations de compte nostro/vostro. Mais c'est une chose que les particuliers dans leur majorité ignorent et qui, à notre avis, ne peut être connue d'une manière générale. Il est donc du devoir de la banque du client effectuant une transaction financière en monnaie étrangère (dans ce cas des dollars américains) qu'elle informe son client qu'un transfert de données vers une banque dans le pays

de la monnaie étrangère peut avoir lieu (ici les Etats-Unis). Néanmoins, dans le cadre de la transaction, la banque de transfert peut tout à fait partir du fait que la banque du mandant a informé en conséquence son client.

Dans les cas où l'institut suisse de crédit a réellement procédé au transfert par l'intermédiaire d'une banque ou d'une filiale aux Etats-Unis et que les autorités américaines, s'appuyant sur une base légale, accèdent à ces données, rien ne s'y oppose du point de vue de la protection des données, car pour que le mandat soit exécuté, le client a consenti à la communication de données à l'étranger. Par contre, une transmission de données ultérieure et de plein gré aux autorités américaines irait à l'encontre des principes du traitement des données (notamment du principe de la proportionnalité). Nous en avons donc conclu qu'une transmission de plein gré des données aux autorités américaines dans le cas présent n'était pas admissible. En revanche, il n'y a pas de violation de la loi sur la protection des données lorsque les autorités américaines consultent les données de transfert transmises aux Etats-Unis dans le cadre de la transaction auprès d'une filiale de l'institut suisse de crédit aux Etats-Unis ou auprès d'une banque partenaire aux Etats-Unis et qu'elle y est légalement légitimée.

Nous soulignons par ailleurs que les sanctions des Etats-Unis ne visent normalement pas les individus, mais les Etats. Pour cette raison, l'institut suisse de crédit a la possibilité d'anonymiser les données de transaction qu'il doit communiquer de telle manière que l'on puisse encore en déduire l'Etat, et éventuellement la ville d'origine du mandant et du destinataire de la transaction, mais pas l'identité propre de ces deux personnes. En procédant ainsi, l'institut suisse de crédit pourrait prouver aux autorités étrangères qu'il respecte les sanctions et en même temps tient compte de manière adéquate de la protection des données.

1.10 International

1.10.1 Coopération internationale

La globalisation de la société engendre des risques en matière de protection des droits et des libertés qui nécessitent des réponses internationales, notamment pour aboutir à la mise en place d'un régime universel de protection des données. Le PFPDT prend ainsi part activement à la collaboration internationale en participant aux travaux du Conseil de l'Europe, à la Conférence européenne des commissaires à la protection des données, aux instances de contrôle communes Schengen et Eurodac, à la Conférence internationale des commissaires à la protection des données et à l'Association francophone des autorités de protection des données.

Conseil de l'Europe

Nous avons pris part aux travaux du comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) et de son bureau. Le comité consultatif a notamment adopté un avis interprétatif des notions de traitement automatisé et de maître du fichier dans le contexte des réseaux mondiaux de télécommunications. Il a en particulier rappelé que la notion de traitement automatisé au sens de la Convention 108 doit être interprétée comme comprenant la collecte effectuée en vue d'un traitement automatisé. En ce qui concerne le maître du fichier ou responsable du traitement, le comité relève qu'il est souvent difficile de déterminer qui est précisément le maître du fichier, car dans la réalité des réseaux mondiaux de télécommunication, plusieurs acteurs sont impliqués et partagent des responsabilités en matière de traitement. Le comité rappelle cependant que le maître du fichier reste légalement responsable envers la personne concernée des opérations de traitement, même si cela suppose qu'il doive ensuite exercer une action récursoire contre un sous-traitant ou co-responsable de traitement. C'est pourquoi lorsque plusieurs acteurs effectuent chacune une partie du traitement, le cas échéant dans des pays différents, il leur incombe de clarifier les responsabilités de chacun, en tenant compte des critères légaux. Le T-PD a également adopté un avis concernant le projet de décision-cadre du Conseil européen relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Après avoir rappelé que la Convention 108 s'applique à la coopération policière et judiciaire en matière pénale, le comité souligne que la

décision-cadre ne peut remettre en cause l'application de la convention et qu'elle devrait plutôt apporter une valeur ajoutée aux principes de base de la protection des données définis dans la convention. Le comité se prononce en outre en faveur d'une application de la décision à l'ensemble des traitements nationaux de données et non pas seulement aux flux transfrontières de données afin de faciliter la coopération policière et judiciaire et d'assurer une protection efficace. Le transfert des données vers des Etats tiers doit respecter les exigences du Protocole additionnel et en particulier si des dérogations sont aménagées au principe du niveau adéquat de protection, elles doivent être définies de manière aussi spécifique que possible, compte tenu de la finalité de la décision-cadre. Le T-PD a aussi adopté un avis concernant la compatibilité de l'application ADAMS (Anti-Doping Administration and Management System) avec les normes du Conseil de l'Europe en matière de protection des données. Il constate que le système de traitement des données mis en place par l'Agence mondiale antidopage soulève plusieurs questions en matière de protection qui touchent notamment à l'information des personnes concernées, au consentement libre et informé et à la base juridique du traitement. Enfin, le T-PD a entamé des travaux relatifs au profilage qui pourraient déboucher sur l'adoption de principes directeurs. Il poursuit ses réflexions sur l'opportunité de développer un instrument juridique consacrant le droit fondamental à la protection des données et prépare un avis interprétatif relatif aux compétences et aux statuts des autorités de contrôle.

Conférence européenne des commissaires à la protection des données

La Conférence européenne des commissaires à la protection des données qui s'est tenue à Larnaca (Chypre) les 10 et 11 mai 2007 a permis aux commissaires des pays parties à la Convention 108 de poursuivre leurs échanges sur certains des principaux thèmes en matière de protection des données (en particulier, dossier électronique du patient, certification, coopération policière et judiciaire, protection des enfants). La Conférence a décidé de renforcer sa structure de coopération dans le domaine de la police et de la justice en créant un groupe de travail avec un président et un vice-président et doté d'un secrétariat permanent.

La Conférence a adopté une déclaration qui concerne le projet de décision-cadre du Conseil européen relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. L'objectif de cette proposition est d'harmoniser les règles de protection des données régissant le traitement des données du 3ème pilier et de faciliter de ce fait l'échange de données dans le cadre de la coopération policière et judiciaire en matière pénale. Il s'agit de garantir un haut niveau de protection des données au sein du 3ème pilier qui devrait être

équivalent à la directive 95/46/CE 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 et respecter les exigences de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) et de son protocole additionnel. Malheureusement les discussions concernant ce texte s'éloignent de cet objectif, notamment du fait qu'une majorité d'Etats veulent limiter le champ d'application de la décision aux échanges d'informations et ne pas couvrir les traitements domestiques qui resteraient régis par les différents droits nationaux. Les commissaires ont ainsi à nouveau exprimé leur préoccupation par rapport à ces développements défavorables au droit de la protection des données et invité les Etats à s'engager en faveur d'un cadre juridique assurant un haut niveau de protection des données (voir annexe 4.18). Les commissaires ont également adopté une opinion relative au principe de disponibilité dans laquelle ils définissent les principes à respecter pour assurer la protection des données et garantir le respect des droits de individus lors de la mise à disposition de données à des fins répressives (voir annexe 4.19).

Groupe de travail «Police et Justice»

Le PFPDT et un représentant des autorités cantonales de protection des données participent également au Groupe de travail «Police et Justice» de la Conférence européenne. Cela leur permet de suivre les développements législatifs autour de l'acquis de Schengen et d'apporter leur contribution au développement du droit européen de la protection des données dans le domaine policier et judiciaire ou de participer à l'élaboration de concepts communs de supervision. Le Groupe de travail a en particulier adopté un avis conjoint avec le Groupe de l'article 29 de la directive européenne 95/46 CE concernant le projet de décision cadre du Conseil sur l'utilisation des données des passagers à des fins répressives. Les commissaires européens rappellent qu'ils soutiennent la lutte contre le terrorisme international et le crime organisé. Ce combat passe nécessairement par la collecte et le traitement de données personnelles. Toutefois, dans la mise en place d'un système PNR européen, les limitations aux droits fondamentaux qui en résulteront doivent être suffisamment justifiées. L'équilibre doit être maintenu entre la garantie des droits fondamentaux et les restrictions indispensables à assurer la sécurité publique. Le projet de proposition cadre prévoit la collecte étendue de données concernant tous les passagers arrivant ou partant d'Europe sans considération du fait qu'ils soient innocents ou suspectés. Ces données seront conservées pour une période de 13 ans et permettront de faire des profilages. Cette proposition est un maillon de plus dans la mise en place d'une société de surveillance sous le couvert de la lutte contre le terrorisme. Les commissaires considèrent que le

projet de décision-cadre est disproportionné et qu'il transgresse les principes de base de la protection des données de la Convention 108. En particulier, la nécessité du traitement est insuffisamment démontrée, la masse de données qui doit être communiquée par les compagnies aériennes est excessive, le filtrage des données sensibles doit incomber au responsable du traitement, le système de «poussée» («push») doit être retenu pour la mise à disposition des données, la durée de conservation des données doit être revue à la baisse, le régime de protection des données, notamment relatif aux droits des personnes concernées et aux obligations des responsables de traitement, est à revoir.

Union européenne

Depuis l'adoption des accords bilatéraux Schengen / Dublin, le PFPDT et un représentant des autorités cantonales de protection des données participent, en tant qu'observateurs, aux travaux de l'Autorité de contrôle commune Schengen (ACC) qui réunit des représentants des autorités nationales de protection des données des Etats Schengen. L'ACC est chargée de surveiller la fonction de support technique du système central d'informations Schengen (SIS) et de vérifier la bonne exécution des dispositions de Convention d'application des Accords de Schengen. Elle est compétente pour l'analyse des difficultés ou l'interprétation survenant dans l'exploitation du SIS. Elle émet en particulier des avis et des rapports sur l'interprétation de la convention d'application des Accords de Schengen. Il s'agit d'un instrument important pour veiller au respect des dispositions de protection des données dans le cadre de la coopération internationale en matière de police et de poursuite pénale. Le PFPDT participe également aux travaux du groupe de coordination Eurodac qui réunit le Contrôleur européen et les autorités nationales de protection des données. Ce groupe a notamment pour tâche de mener des inspections conjointes du système Eurodac, d'examiner les problèmes de protection des données dans le cadre de l'exploitation du système, d'émettre des avis concernant l'interprétation des dispositions légales et d'adresser des recommandations.

Conférence internationale des commissaires à la protection des données

La 29ème Conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue à Montréal du 25 au 27 septembre 2007. Sous le thème «Terra Incognita, les horizons de la protection de la vie privée», la conférence a réuni quelque 600 participants venus du monde entier. Ainsi les commissaires à la protection des données ont pu échanger avec les représentants de la société civile (gouvernement, administration, économie, science et recherche, consommateurs, organisations inter-

nationales gouvernementales et non gouvernementales) autour des enjeux actuels de la protection des données que sont notamment la circulation transfrontière des données, l'informatique ubiquiste, les politiques de sécurité publique, la protection de la vie privée des jeunes ou les recoupements entre la loi et la technologie. Ces échanges ont permis de tirer des enseignements pour les actions des autorités de protection des données dans les années à venir et contribuer au renforcement de la collaboration internationale en matière de protection des données (http://www.conference-vieprivee2007.gc.ca). La conférence a confirmé le constat des années précédentes, à savoir que la surveillance est une réalité, que les technologies remettent en cause le droit à la vie privée, que l'informatique ubiquiste et notamment la bioinformatique transforme l'être humain en système de traitement des données et que les réponses juridiques actuelles sont insuffisantes face au traçage systématique des individus. Il est impératif de définir à nouveau ce que nos sociétés veulent en matière de respect de la vie privée et de la protection des données.

Les commissaires à la protection des données et à la vie privée ont, dans le cadre de leur conférence à huis clos, adopté 4 résolutions. La première résolution concerne l'urgence d'établir des normes mondiales visant la protection des données des passagers dont se serviront les gouvernements pour appliquer les lois et assurer la sécurité transfrontalière. Cette résolution fait suite à une résolution que nous avions proposée lors de la 25ème conférence internationale à Sydney en septembre 2003. La deuxième résolution adoptée appelle à l'élaboration de normes liées à la protection de la vie privée concernant l'utilisation et la mise en place de technologies. Ces spécifications techniques et organisationnelles visent à mettre en pratique les exigences juridiques. Ces normes doivent être élaborées en collaboration avec les autorités de protection des données. Dans une troisième résolution, les commissaires appellent au renforcement de la coopération internationale. Enfin, une quatrième résolution vise à l'amélioration de l'organisation de la conférence internationale et notamment au développement d'un site Web tel que décidé lors de la 27ème conférence qui s'est tenue à Montreux en 2005.

Nous avons eu également l'occasion de présenter à nos collègues un premier rapport d'évaluation de la concrétisation de la déclaration finale de la 27ème conférence (déclaration de Montreux) qui appelait au renforcement du caractère universel du droit à la protection des données, notamment à la préparation d'un instrument juridique universel contraignant (voir notre 13ème rapport d'activités, ch. 9.2 et annexe 11.2). Cette évaluation s'est faite sur la base d'un questionnaire que nous avons adressé à l'ensemble des autorités nationales de protection des données ayant participé à la conférence de Montreux. Dans ce rapport, nous avons pu établir que dans l'année qui a suivi l'adoption de la déclaration de Montreux, une large diffusion de la déclaration

de Montreux, notamment par le biais de l'Internet, a été assurée. Il est cependant difficile de mesurer l'impact de cette diffusion et notamment d'évaluer dans quelle mesure les destinataires potentiels ont pris connaissance de la déclaration et l'ont intégrée dans leurs activités. Si la déclaration a été portée à la connaissance de nombreux acteurs nationaux et internationaux, il semble néanmoins que peu d'entre eux ne se l'approprient encore comme devant faire partie de leurs propres objectifs. Les actions plus ciblées ont eu un certain effet. Ainsi plusieurs autorités sont intervenues auprès des ministres participant au Sommet mondial de la société d'information pour les inviter à soutenir l'adoption d'une référence à la protection des données dans les actes du sommet. Il en va de même pour la déclaration finale du XIème sommet de la Francophonie qui s'est tenu à Bucarest en septembre 2006.

La réalisation des objectifs de la déclaration est un processus dynamique qui nécessitera du temps, de la patience et de la persévérance. La déclaration a eu un effet positif et joué un rôle moteur pour de nombreuses initiatives. La conscience de l'universalité de la protection des données n'a jamais été aussi présente, mais elle demeure des plus fragiles face aux priorités que sont devenues la sécurité et la surveillance dans le cadre de la lutte contre le terrorisme et la criminalité organisée. Les autorités de protection des données prennent de plus en plus conscience de leur rôle dans la société actuelle et de l'importance d'être présentes et actives de manière coordonnée dans la défense du droit à la protection des données. Le nombre de pays européens et extra-européens, notamment ceux réunis au sein de la francophonie et de la conférence ibéro-américaine, qui se montrent favorables à un instrument universel contraignant, est en constante augmentation. L'idée de la convention universelle progresse. Toutefois sa réalisation ne sera pas aisée et sera sujette à de fortes résistances. Des initiatives concurrentes se sont développées. Il conviendrait de coordonner ces initiatives afin qu'elles soient complémentaires les unes aux autres et ne remettent pas en cause l'objectif principal que nous avons voulu avec la déclaration de Montreux, à savoir une cadre universel contraignant en matière de protection des données et de respect de la vie privée. Les commissaires ont accepté à l'unanimité notre rapport et nous ont chargés de présenter un rapport complémentaire lors de la 30ème Conférence internationale qui se tiendra à Strasbourg en octobre 2008.

Association francophone des autorités de protection des données

Le 24 septembre 2007 s'est tenue à Montréal la première conférence des commissaires à la protection des données de la Francophonie (http://www.cai.gouv.qc.ca/CCPDF). Nous y étions représentés. La conférence portait sur les liens d'interaction entre la protection des données personnelles, la démocratie et le développement.

Cette conférence a permis un dialogue entre des Etats ayant déjà une longue expérience en matière de protection des données, notamment dotés d'autorités de protection des données et les Etats émergents qui viennent d'adopter une loi, à l'instar du Burkina Faso, ou qui s'apprêtent à démarrer dans le processus législatif. L'objectif était également de créer un programme de coopération et d'échange entre autorités de protection des données de la francophonie en vue de partager les expériences concrètes dans ce domaine. La conférence a débouché sur la création de l'Association francophone des autorités de protection des données. L'Association est présidée par le président de la commission d'accès à l'information du Québec. Nous en assumons une des deux vice-présidences. La CNIL (France) en assure le secrétariat. L'Association est soutenue par l'Organisation Internationale de la Francophonie dont elle partage pleinement l'objectif d'œuvrer pour la paix, la démocratie et le développement du droit en apportant son soutien à l'Etat de droit et aux droits de l'homme. Parmi les objectifs de l'Association figurent l'accroissement de l'efficacité de ses membres dans la promotion de la protection des données, l'échange d'informations entre autorités de protection des données, la constitution de pôles d'expertise et d'échange d'expériences, la consolidation de la protection des données personnelles en tant que facteur de la promotion de l'Etat de droit et du développement démocratique. L'Association veut en particulier aider les Etats émergents dans la mise en place de leur législation et de leurs autorités de protection des données. Elle favorisera le rapprochement des législations et contribuera ainsi à l'effectivité du droit sur le plan transfrontalier, à la lisibilité et à la flexibilité dans les méthodes de mise en œuvre. Elle s'engagera également en vue de la reconnaissance du droit universel à la protection des données.

1.10.2 Groupe de travail international sur la protection des données dans le domaine des télécommunications

Parmi les thèmes de discussion figurant à l'agenda de la 42ème réunion du groupe de travail en automne 2007 à Berlin figuraient la protection des données lors de la diffusion de contenus numériques par les médias et la télévision numérique ainsi que l'utilisation de billets électroniques dans les transports publics.

Nous avons participé à la 42ème réunion du «Groupe de Berlin» (International Working Group on Data Protection in Telecommunications, IWGDPT), qui s'est tenue du 4 au 5 septembre 2007. Ce groupe de travail a été mis sur pied lors de la Conférence internationale des Commissaires à la protection des données de 1983 déjà, sur l'initiative du délégué à la protection des données de Berlin, qui le préside encore à l'heure actuelle.

La discussion sur le thème de la protection des données lors de la diffusion de contenus numériques par les médias a abouti à l'adoption d'un document de travail contenant des recommandations; en effet, la télévision numérique interactive offre de nouvelles possibilités et de nouveaux services à ses utilisateurs, mais comporte aussi des risques pour la sphère privée. Les traitements de données sont le plus souvent effectués sous le contrôle des fournisseurs et manquent de transparence pour les utilisateurs. La consommation des contenus numériques peut mener à la création de profils de la personnalité contenant des informations très sensibles sur les intérêts et les préférences des clients. C'est la raison pour laquelle le groupe de travail demande qu'on préserve, même à l'ère de la télévision numérique, la possibilité d'utiliser ces services de manière anonyme. Il convient de proposer, au moins comme option, des modes de paiement anonymes qui n'occasionnent pas de frais supplémentaires. Si des traitements de données sont effectués, les téléspectateurs doivent être préalablement informés sur l'étendue, le but et le lieu du traitement ainsi que sur la durée de conservation des données.

Le groupe s'est également penché sur le thème de l'utilisation de plus en plus fréquente de billets électroniques dans les transports publics. Très souvent, ces systèmes fonctionnent avec des cartes à puce personnalisées qui permettent de payer pour l'utilisation des moyens de transport, mais aussi pour d'autres prestations annexes telles que le parcage. Il peut en résulter des informations qui permettent de dire qui s'est trouvé quand et à quel endroit (profils de déplacement). Le groupe de travail demande que les exigences de la législation sur la protection des données soient prises en compte déjà au moment de la conception de tels systèmes de billetterie électronique. Comme pour la télévision numérique, il doit également être possible d'utiliser les prestations de manière anonyme (avec paiement en espèces ou prépaiement) dans les transports publics, ceci sans être pénalisé du point de vue financier. Les entreprises de transport effectuant des traitements de données personnelles doivent respecter le principe d'économie des données et réduire au minimum la durée de conservation des données. D'autre part, tous les traitements de données doivent être absolument transparents pour les clients.

Les documents publiés par le groupe se trouvent sous www.iwgdpt.org

2 Principe de la transparence

2.1 Premières expériences avec le principe de la transparence

Le principe de la transparence est en train de s'établir au sein de l'administration fédérale. L'année passée, les offices fédéraux ont, pour deux tiers des demandes reçues, accordé un accès complet ou au moins partiel aux documents. En ce qui concerne les demandes en médiation, nous avons dans presque tous les cas réussi à obtenir un résultat plus favorable pour le requérant. Ce sont surtout les journalistes qui recourent aux possibilités de la loi sur la transparence.

Depuis le 1er juillet 2006, les citoyens ont un droit d'accès aux documents officiels de l'administration fédérale, des Services du Parlement et d'organismes ou personnes de droit public ou de droit privé qui sont soumis à la loi sur la transparence. Si un de ces organismes refuse entièrement ou partiellement sa demande d'accès, le requérant peut déposer chez nous une demande en médiation. Le premier bilan sur une année entière montre une image à tous points de vue positive: la population utilise de plus en plus les possibilités de la loi sur la transparence et reçoit dans la majorité des cas aussi l'accès aux documents demandés.

Demandes d'accès reçues auprès des offices fédéraux et départements

Les organes qui sont soumis à la loi sur la transparence doivent nous communiquer chaque année combien de demandes d'accès ils ont reçues et comment ils ont tranché. Ainsi, en 2007 les autorités fédérales auraient reçu 249 demandes d'accès (cf. la statistique au chiffre 3.5). Dans 147 cas, les autorités ont accordé un accès sans restriction et dans 20 cas un accès limité. Dans 82 cas, l'accès aux documents a été refusé.

Ceci nous permet de conclure ce qui suit:

- Pour deux tiers des demandes d'accès déposées, un accès sans restriction ou un accès limité ont été accordés. On parle d'un accès limité lorsque certaines parties du document en question sont caviardées et/ou si des noms de personne ont été anonymisés. Pour un peu moins du tiers des demandes, l'accès a été complètement refusé.

- Le nombre élevé de refus ainsi que le nombre relativement bas d'accès limités permettent de conclure une fois de plus que les autorités fédérales font (trop?) peu usage de la possibilité d'accorder un accès limité. Il semble que l'on préfère refuser complètement l'accès plutôt que de vérifier s'il serait possible d'accorder un accès limité. La loi sur la transparence prévoit explicitement cette possibilité et les unités administratives devraient dans le cadre de l'application du principe de proportionnalité davantage veiller à accorder à un requérant au moins un accès à une partie du document dans les cas où un accès sans restriction ne peut pas être accordé.

- De nombreuses unités administratives n'ont, selon leurs propres indications, pas reçu de demandes en 2007, d'autres nous signalent qu'ils ont reçu plus de 30 demandes. Une des explications possibles pour ces différences importantes est que certains offices sont plus exposés au public que d'autres, en fonction des thèmes et des matières qu'ils traitent et reçoivent donc plus ou moins de demandes d'accès. Dans ce contexte, la question se pose néanmoins de savoir si toutes les unités administratives reconnaissent effectivement comme telles les demandes reçues et si elles sont saisies de manière systématique. Sur la base de réactions que nous avons reçues des offices, nous avons en outre pu constater qu'il existe des difficultés à distinguer une demande d'accès selon la loi sur la transparence d'une demande générale de renseignements. La loi sur la transparence ne se prononce pas clairement sur cette question. En principe, nous tendons à dire qu'une saisie correcte et systématique de toutes les demandes d'accès aboutirait à un nombre bien plus élevé de demandes rapportées.

- Il n'a pas été possible d'obtenir des informations fiables sur les émoluments perçus dans le cadre des accès accordés ainsi que sur la charge de travail que ceux-ci occasionnent dans les offices et départements. Les informations qui nous ont été transmises ne sont pas assez significatives. Il est néanmoins possible d'en dégager les tendances suivantes: dans la grande majorité des cas, aucun émolument n'est demandé pour l'accord de l'accès. En ce qui concerne la charge de travail occasionnée par la loi sur la transparence, les indications des divers offices et départements sont très divergentes (pour autant que la charge de travail nous ait été communiquée): on y trouve de tout, de la charge de travail minime à une charge de travail très importante. Afin de pouvoir procéder à l'évaluation demandée par la loi sur la transparence, il est absolument nécessaire que ces informations soient dorénavant saisies de manière plus correcte et systématique.

Demandes en médiation

Si un requérant voit sa demande d'accès refusée ou limitée à une partie des documents ou s'il ne reçoit pas de réponse de l'autorité dans les délais prévus par la loi, il peut déposer chez nous une demande en médiation. Alors que pendant les six premiers mois qui ont suivi l'entrée en vigueur de la loi sur la transparence (1er juillet 2006), nous n'avons reçu que six demandes en médiation, le nombre est passé à 36 en 2007 (cf. la statistique au ch. 3.5).

En 2007, nous avons pu clore 26 demandes en médiation. Dans 7 cas, nous avons conclu que la loi sur la transparence n'était pas applicable. Dans deux cas, nous avons pu trouver une solution consensuelle avec les parties impliquées et dans 14 cas nous avons, faute d'avoir pu trouver une solution à l'amiable, émis des recommandations. Ces recommandations se trouvent dans les annexes 4.6 et 4.17. Dans 3 cas, l'accès aux documents a encore été accordé par l'office par la suite.

Ces chiffres permettent de conclure ce qui suit:

- Dans 102 cas, les autorités ont complètement refusé l'accès (82) ou ne l'ont accordé que de manière limitée (20). 36 demandes en médiation ont été déposées chez nous. Cela signifie donc que nous avons reçu une demande en médiation dans un tiers des demandes d'accès entièrement ou partiellement refusées.

- Dans 14 des 16 cas de médiation, nous avons réussi à trouver une solution plus favorable pour le requérant (à savoir un accès plus large que ce qui avait à l'origine été accordé par l'office fédéral).

- A deux exceptions près, toutes nos recommandations ont été acceptées par les requérants et les offices fédéraux; dans deux cas, le requérant a exigé que l'autorité rende une décision (nous ne savons pas encore à l'heure actuelle si un recours a été déposé auprès du Tribunal administratif fédéral).

- Dans trois cas, les procédures en médiation ont pu être suspendues parce que les autorités sont revenues sur leur décision et ont quand même accordé l'accès aux documents souhaités. Ces cas montrent que l'introduction du principe de transparence dans l'administration fédérale a mené à une situation où l'on choisit plutôt de publier un document que de le retenir. Cette évolution nous est également confirmée lors de nos discussions répétées avec les offices et les départements.

- Une année et demie après l'introduction de la loi sur la transparence, nous pouvons constater que l'institution de la médiation est fortement utilisée par les citoyens. En contemplant le pourcentage de réussite des demandes, nous pouvons faire un premier constat intermédiaire: le but poursuivi par le législateur, à savoir d'éviter les procédures judiciaires longues et coûteuses par la mise en place d'un organe de conciliation indépendant et interne à l'administration, a été atteint.

Finalement, nous pouvons également constater ce qui suit:

- Un des gros problèmes dans la procédure d'accès interne à l'administration est le retard important qui intervient dans le traitement des demandes en médiation. Ces retards sont regrettables et sont en contradiction avec l'esprit du principe de la transparence. C'est notamment dans le cadre des médiations qu'on peut régulièrement constater que les offices non plus ne respectent pas toujours les délais fixés par la loi pour l'appréciation d'une demande d'accès.

- N'importe qui peut déposer une demande d'accès et par conséquent aussi une demande en médiation. Il n'est pas nécessaire de justifier d'un intérêt, ni dans le premier, ni dans le deuxième cas. Ceci pourrait être une raison qui explique le nombre relativement élevé de demandes en médiation reçues.

- Il s'avère que ce sont surtout les journalistes, les avocats et les représentants de milieux intéressés qui savent tirer profit des avantages de la loi sur la transparence. Ainsi, les demandes d'accès et les demandes en médiation sont plus souvent déposées par des représentants de milieux intéressés (par exemple par une organisation de défense des consommateurs dans le cas de l'étude faite par l'EPF sur les acides gras trans) ou par des entreprises concurrentes ou leurs avocats (par ex. dans le cas du contrat souscrit par l'OFSP pour l'achat d'un vaccin prépandémique ou la recommandation relative à l'homologation de médicaments). Le corps de métier qui dépose le plus de demandes en médiation est cependant celui des journalistes (11).

- Les raisons les plus avancées pour justifier le refus ou la limitation d'une demande d'accès ont été le secret d'affaires ou de fabrication, les relations internationales ou les décisions politiques ou administratives qui n'ont pas encore été prises.

- À notre avis, les autorités ont tendance à se référer à une disposition d'exception pour justifier leur refus d'accorder l'accès afin d'éviter de devoir fournir une justification plus détaillée, ceci aussi bien lors de l'appréciation des demandes d'accès que lors de la médiation. Les offices semblent nous faire confiance que nous prendrons une décision dans ce sens dans le cas d'une médiation.

Cette manière de procéder est insatisfaisante et choquante pour les requérants. Ceux-ci devraient au moins être en mesure de comprendre pour quelles raisons une autorité fait valoir une disposition d'exception. Nous tenons également à rappeler ici que l'intention du législateur n'était pas que le PFPDT soit une instance judiciaire anticipée, mais qu'il joue en premier lieu un rôle de médiateur, ce qui signifie qu'il s'efforce de trouver une solution qui soit acceptable pour les deux parties.

3 Préposé fédéral à la protection des données et à la transparence

3.1 WebDatareg: le nouveau programme d'annonce et de consultation en ligne des fichiers

Conformément au nouvel article 11a de la LPD révisée, le préposé tient un registre des fichiers accessible en ligne. Appuyé par la Chancellerie fédérale, nous avons tout d'abord défini puis réceptionné un programme trilingue pour la gestion en ligne des annonces de fichier par les organes fédéraux et les personnes privées. Le temps investi pour la saisie, la mise à jour et la recherche s'en trouvera fortement réduit pour tous les acteurs concernés. Fin 2007 et début 2008, nous avons mis sur pied plusieurs cours de formation à l'attention des organes fédéraux, afin que ces derniers puissent au besoin mettre à jour leurs annonces existantes avant la mise en ligne du registre sur Internet, prévue d'ici à l'été 2008. On peut noter que les entreprises disposeront alors également d'une possibilité d'annonce en ligne de leurs fichiers.

Dans le cadre de la révision LPD adoptée par le Parlement le 24 mars 2006, le premier alinéa de l'article 11a sur le registre des fichiers prévoit désormais que «le préposé tient un registre des fichiers accessible en ligne. Toute personne peut consulter ce registre». Avec l'appui de la Chancellerie fédérale, nous avons tout d'abord établi le cahier des charges d'un nouveau programme basé sur le Web pour la gestion et consultation des données contenues dans ce registre. Ce nouveau programme complètement trilingue s'appuie sur le nouvel environnement Microsoft.NET, avec une base de données relationnelle entièrement renormalisée sous SQL-Server. Afin de garantir la sécurité des accès Internet, une réplique des données à publier est assurée par un service exclusif de synchronisation à partir des données de référence gérées au sein du réseau interne de la Confédération.

Dans un premier temps, le rôle Administrateur a été mis en production chez nous, afin que nous puissions gérer les nouvelles annonces et bien sûr toutes les annonces existantes reprises de l'ancien registre Access. Dans un deuxième temps (fin 2007/ début 2008), nous avons offert une formation bilingue à une centaine de personnes provenant des organes fédéraux annonceurs, afin que ces derniers puissent saisir leurs nouvelles annonces à l'aide du nouveau programme et au besoin modifier les données de leurs anciennes annonces. Dans un troisième temps, nous allons envoyer une copie des annonces existantes à toutes les personnes privées (entreprises) concernées, en leur demandant de bien vouloir vérifier l'exactitude des données an-

noncées. En outre, ces entreprises disposeront d'un programme d'annonce en ligne analogue à celui fourni aux organes fédéraux; toutefois les données d'annonce nous seront transmises par voie de messagerie électronique sous la forme de fichiers PDF et XML. Après authentification de l'annonceur, nous serons ainsi à même d'importer facilement les données XML reçues dans le registre, et nous assurerons au passage la traduction de la dénomination et du but du fichier dans les deux autres langues nationales.

En fait, toutes ces étapes ont pour ultime finalité la mise à disposition sur Internet d'une application de recherche et de consultation des fichiers annoncés et contenus dans le registre. La publication officielle de ce registre sur Internet devrait avoir lieu au début de l'été 2008.

3.2 Deuxième Journée européenne de la protection des données

Le 28 janvier 2008, nous nous sommes associés à la Radio Suisse Romande et à Schweizer Radio DRS pour organiser la deuxième Journée européenne de la protection des données. L'objectif du Conseil de l'Europe, qui est de sensibiliser la population, a pu être atteint grâce à la diffusion de nombreuses émissions ainsi qu'aux spécialistes qui ont répondu aux questions des auditeurs et des auditrices.

Les deux stations de radio RSR et DRS ont saisi l'occasion qui leur était offerte lors de cette deuxième Journée européenne de la protection des données pour aborder les questions que pose au quotidien la protection de la personnalité, et ce au cours de diverses émissions: de la cybersanté («e-Health») à la question fondamentale du genre de données disponibles sur une personne et de l'utilisation qui en est faite et par qui, en passant par les puces RFID et le traçage de données sur Internet, notamment sur le Web 2.0. Le préposé fédéral à la protection des données et à la transparence, Hanspeter Thür, a participé à plusieurs discussions sur DRS1, alors que son suppléant, Jean-Philippe Walter, est intervenu pour sa part sur La 1ère et Couleur 3.

En parallèle à ces émissions, les collaborateurs du PFPDT, experts en matière de protection des données, ont répondu aux questions du public sur une hotline ainsi que sur un forum Internet. Quelque 200 questions ont été posées. Elles ont montré le large éventail des préoccupations des citoyens quant à la protection de leur sphère privée: formulaires d'inscription pour la location d'appartements, surveillance par vidéo émanant de voisins, demande de références par l'employeur, accès aux dossiers du personnel, accès aux antécédents médicaux, remise des mêmes antécédents médicaux, carte de santé ou encore risques liés à l'utilisation des cartes de crédit, pour ne citer que quelques exemples. Ces contacts que nous avons eus avec différents segments

de la population ont aussi confirmé, du moins partiellement, le point de vue du Conseil de l'Europe, selon lequel les citoyens sont relativement peu informés sur la protection des données, sur les risques encourus quotidiennement en relation avec les données personnelles et sur les droits des personnes. Nous œuvrerons à l'avenir aussi pour qu'une plus grande information se fasse au bénéfice de la population.

3.3 Publications du PFPDT – nouveaux titres

Cette année écoulée également a été caractérisée par un élargissement de l'éventail des informations que nous proposons sur notre site web. Nous avons entre autres publié des explications concernant les mesures de sécurité à prendre lors de l'utilisation de réseaux sans fil, les «listes noires» dans l'hôtellerie et la restauration ainsi que bien sûr la version révisée de la loi sur la protection des données.

Le 1er janvier 2008, la loi fédérale révisée sur la protection des données est entrée en vigueur. Les principaux changements introduits par cette révision sont commentés dans la rubrique Thèmes – Protection des données – Autres thèmes – Révision de la loi fédérale sur la protection des données (LPD).

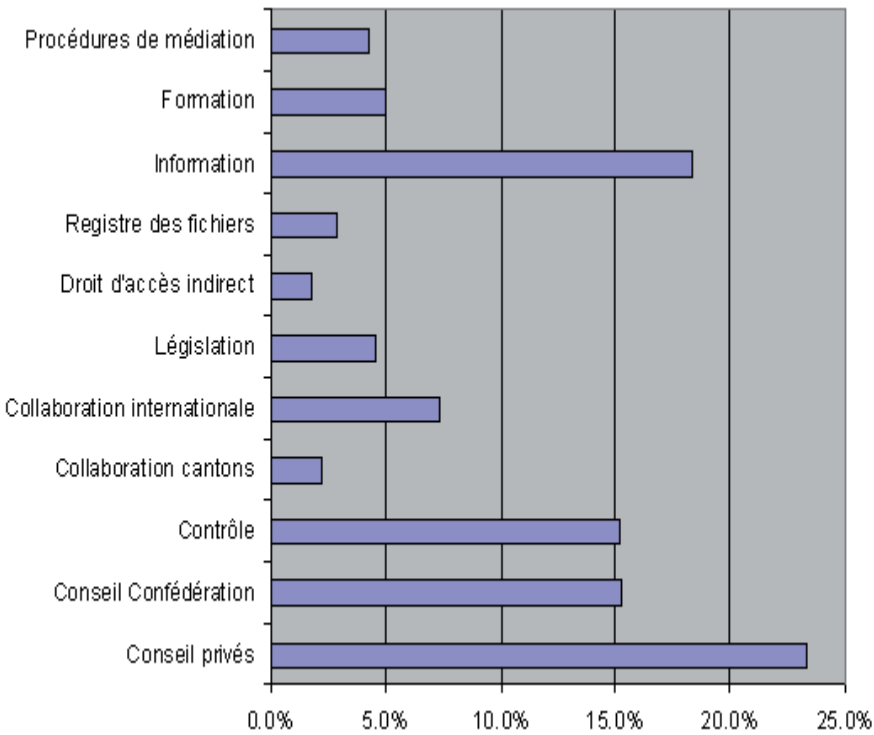
Les réseaux Wi-Fi, autrement dit les réseaux sans fil, se répandent de plus en plus. Malheureusement, la prise de conscience des risques d'atteinte à la sphère privée liés à l'utilisation de ces réseaux ne suit pas le mouvement. Nous avons publié quelques conseils pour des mesures de sécurité minimales dans la rubrique Thèmes – Protection des données – Internet – WLAN. De plus, nous avons également inclus un article sur ce thème dans notre newsletter «datum» (édition 02/2007).

L'hôtellerie et la restauration sont régulièrement confrontées à des clients qui se comportent de manière inconvenante et se rendent coupables de grivèlerie, de dommages à la propriété ou même de comportement agressif envers d'autres clients. Dans ce contexte, on nous a souvent demandé si les restaurateurs, gérants de clubs et hôteliers pouvaient mettre sur pied une banque de données permettant de les mettre en garde contre les agissements de telles personnes, et si oui à quelles conditions. Dans la rubrique Thèmes – Protection des données – Autres thèmes – Listes noires, nous expliquons quels sont les points auxquels prêter attention en ce qui concerne la protection des données lors de la création de telles listes (cf. également l'annexe 4.1).

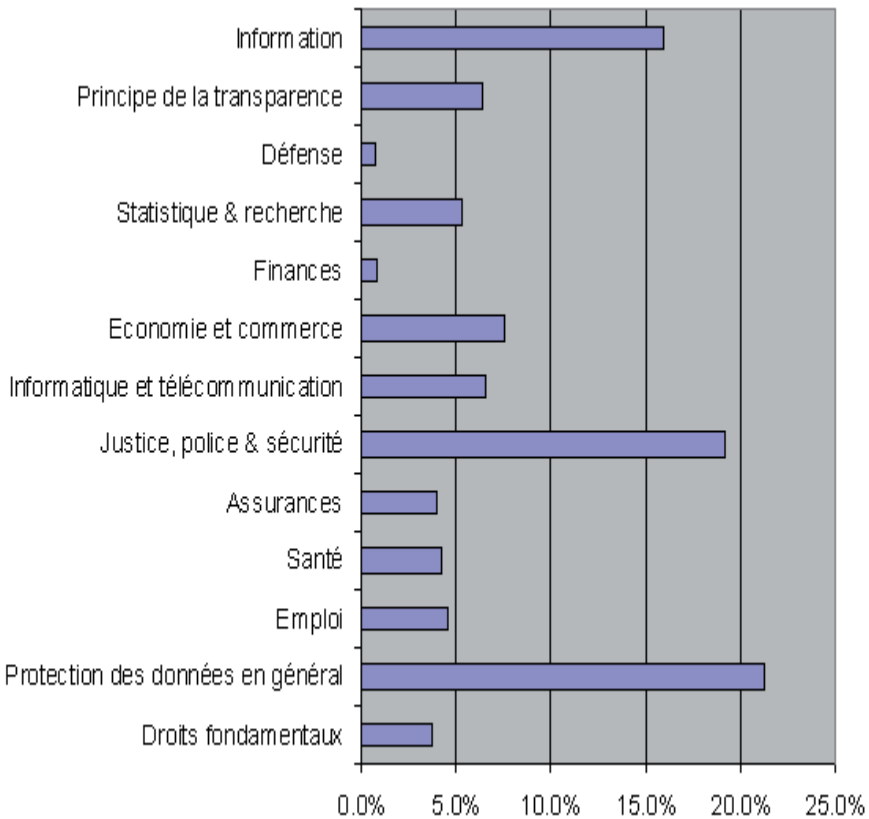
Notre newsletter «datum» (édition 02/2007) contient en outre un article sur la miniaturisation des appareils de surveillance et ce qu'on appelle le «pervasive computing», c'est-à-dire l'informatisation complète de notre vie quotidienne («De Big Brother à Little Brother»).

3.4 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2007 au 31 mars 2008

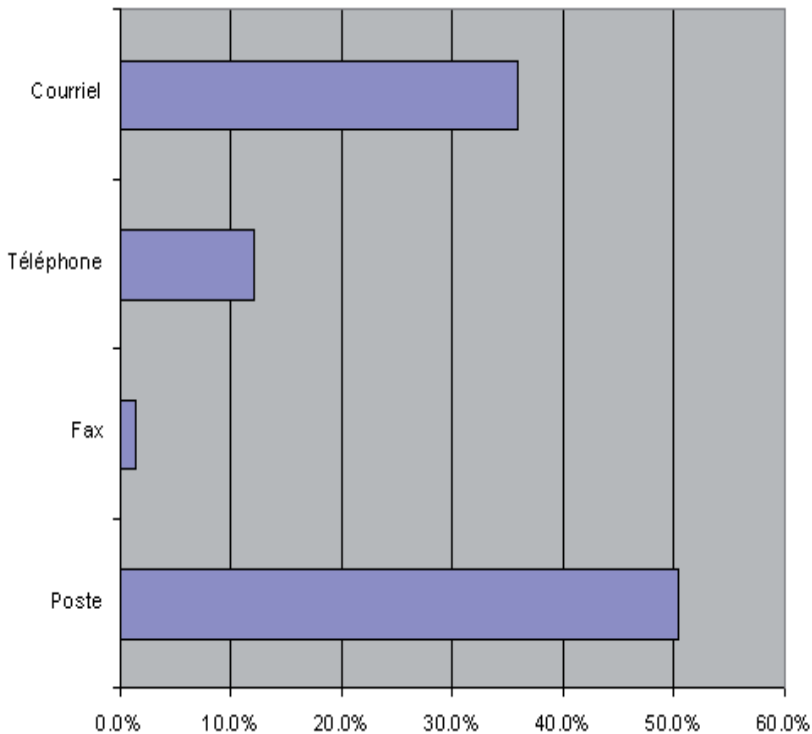
Charge de travail par tâches



Charge de travail par domaines



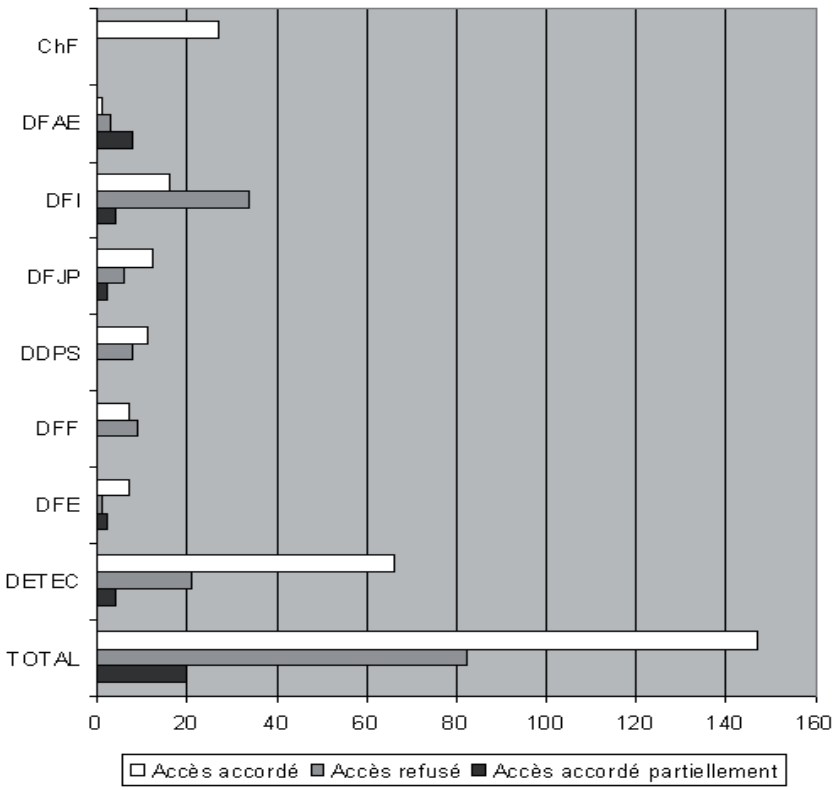
Provenance des demandes



3.5 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2007 au 31 décembre 2007)

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé
ChF (dont PFPDT)	27 (27)	27 (27)	0	0
DFAE	12	1	3	8
DFI	54	16	34	4
DFJP	20	12	6	2
DDPS	19	11	8	0
DFF	16	7	9	0
DFE	10	7	1	2
DETEC	91	66	21	4
TOTAL	**249**	**147**	**82**	**20**

Traitement des demandes d'accès



Nombre de demandes de médiation par catégories de requérant en 2007

Catégorie de requérant	Nombre
Personnes privées (ou requérant ne pouvant pas être attribué de manière précise)	12
Médias/journalistes	11
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	5
Avocats	6
Entreprises	2
Total	36

3.6 Secrétariat du Préposé fédéral à la protection des données et à la transparence

Préposé fédéral à la protection des données et à la transparence:

	Thür Hanspeter, Fürsprecher
Suppléant:	Walter Jean-Philippe, Dr. iur.

Secrétariat:

Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité 1:	9 personnes
Unité 2:	12 personnes
Unité 3:	1 personne
Chancellerie:	3 personnes

4 Annexes

4.1 Explications sur les «listes noires»

Les hôteliers et les restaurateurs sont régulièrement confrontés à des clients qui se comportent de manière inadmissible, ne payent pas leurs factures, causent des dégâts ou se montrent agressifs envers d'autres clients. Des aubergistes, des gérants de club et des hôteliers lésés se sont adressés de manière répétée au Préposé fédéral à la protection des données et à la transparence pour lui demander s'ils peuvent créer une banque de données en vue d'éviter des surprises désagréables avec de tels délinquants et si oui, à quelles conditions.

Il est compréhensible que les responsables d'établissements d'hôtellerie-restauration et d'établissements apparentés veuillent enfin empêcher des personnes au comportement inadmissible de nuire et protéger leurs établissements contre de tels clients. La création d'une banque de données par des particuliers (dont font aussi partie les restaurateurs, les hôteliers, etc.) et le fait qu'un groupe entier de personnes puisse accéder à ces données ne sont pas sans poser problème du point de vue du droit de la protection des données.

Contexte légal

Toute gestion de données personnelles, donc aussi le fait de collecter des informations sur des délinquants et de les mettre en partage dans une banque de données, constitue un traitement de données au sens de la loi fédérale sur la protection des données (LPD). Cette dernière prévoit que la personne qui traite des données doit disposer d'un motif justificatif pour procéder au dit traitement. Sont réputés motif justificatif le consentement de la personne concernée, un intérêt prépondérant privé ou public ou une loi. Il est peu probable que les délinquants acceptent de figurer sur une liste noire. En outre, il n'existe pas de loi obligeant les exploitants d'hôtels et de restaurants à gérer une telle banque de données. En revanche, l'intérêt prépondérant privé de ces exploitants peut justifier un traitement de données personnelles.

La personne qui procède au traitement des données doit par ailleurs respecter les principes généraux de la LPD. Elle doit donc

- informer clairement les personnes concernées du but et des conditions du traitement des données (principes de la transparence et de la bonne foi);

et peut

- traiter uniquement les données personnelles appropriées et nécessaires pour atteindre le but poursuivi par le traitement des données (principe de la proportionnalité) – il doit exister un rapport raisonnable entre le résultat recherché et les moyens utilisés;
- traiter les données dans le seul but qui est annoncé lors de leur collecte, qui ressort des circonstances ou qui est prévu par une loi (principe de la finalité).

Règles pour le traitement des données

Pour garantir une procédure claire et juridiquement irréprochable, il est recommandé d'élaborer un ensemble de règles pour le traitement des données, ensemble qui s'appliquera à toutes les parties concernées et protègera les droits des personnes dont les données sont saisies.

Ces règles comprennent les points suivants:

- Finalité. La finalité du traitement des données doit être définie: dans le cas d'espèce, l'enregistrement des coordonnées de personnes ayant eu des comportements manifestement inadmissibles dans un établissement d'hôtellerie-restauration aurait pour finalité d'empêcher que d'autres exploitants subissent des préjudices semblables.
- Conditions d'un enregistrement dans la banque de données. Il convient de préciser qu'un enregistrement dans la banque de données ne peut avoir lieu qu'en cas de dommages non payés ou de tout autre préjudice résultant d'un comportement manifestement inadmissible.
- Données personnelles enregistrées. Il est primordial de définir les données personnelles destinées à être enregistrées dans la banque de données. Il paraît à cet égard suffisant de ne saisir que les coordonnées de la personne concernée et le motif de l'enregistrement (nature du préjudice), de même qu'un identifiant qui permette de prendre éventuellement contact avec la personne qui a introduit les données.
- Information. Les clients doivent être clairement informés du but et des conditions de la collecte des données et de leur enregistrement dans la banque de données. Ces informations peuvent par exemple figurer dans des conditions

générales, celles-ci étant portées à la connaissance des clients lors de la réservation sur Internet et/ou clairement affichées dans la chambre d'hôte. Si la réservation n'a pas été faite par le biais d'Internet, ces informations figureront sur le formulaire à remplir auprès de l'exploitant.

- Garantie du droit d'accès et de rectification. La personne qui gère un fichier doit garantir que les personnes concernées puissent faire valoir leur droit d'accès et de rectification des données. Cela signifie que les clients dont les données ont été effectivement enregistrées dans la banque de données, et donc mises à la disposition d'autres hôteliers-restaurateurs, doivent être dûment informées afin de pouvoir exercer leur droit d'accès et de rectification.
- Accès à la banque de données. Une telle banque de données équivaut à une liste noire et ne doit en aucun cas être publiquement accessible. L'accès au fichier doit être limité à un groupe de personnes clairement défini et à des demandes concrètes. Un accès aux listes complètes ne saurait être accordé.
- Durée de conservation des données. Une durée de conservation de deux ans, c'est-à-dire la destruction des données après deux ans (à compter du dernier incident enregistré pour une personne déterminée), paraît conforme au principe de la proportionnalité.
- Mesures de protection appropriées. Les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

Vous trouverez d'autres informations sur la protection des données sur notre site web www.leprepose.ch.

4.2 Explications relatives à «Voice over IP» et la protection des données

Définition et problématique

L'utilisation de la téléphonie par Internet (Voice over IP, VoIP) a connu un énorme essor ces derniers temps. La transmission vocale ne se fait plus à travers les réseaux téléphoniques classiques séparés (réseau téléphonique commuté, RNIS) mais avec commutation de paquets par Internet. Cela signifie que:

- La communication vocale se fait sous forme numérique
- La communication utilise les canaux Internet usuels

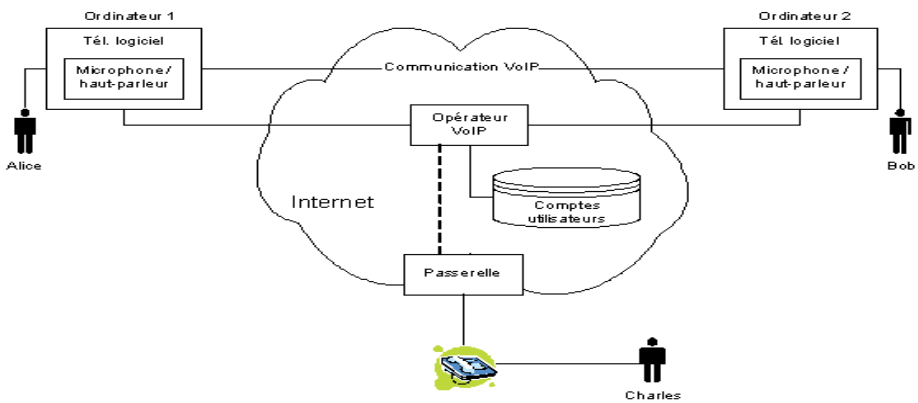
Ces deux caractéristiques importantes augmentent le risque qu'une conversation téléphonique soit illicitement interceptée, vu qu'il est plus facile d'accéder aux données transmises et que les données numériques facilitent une analyse automatisée.

La forme numérique présente en outre l'inconvénient que les communications, p.ex les traces électroniques laissées sur un serveur ou sur le PC d'un utilisateur, peuvent facilement être copiées.

Objectif

L'objectif de ce document est de montrer les principaux risques qui existent en matière de protection des données lors d'une utilisation de VoIP et de donner des conseils permettant d'améliorer cette protection, aussi bien pour les utilisateurs que pour les prestataires. Dans ce contexte, nous avons examiné les principaux téléphones logiciels qui sont disponibles gratuitement sur le marché.

Schéma de principe d'une communication:



Conseils du PFPDT

Lors de notre étude des divers téléphones logiciels proposés sur le marché, nous avons comme prévu constaté des points forts et des points faibles en ce qui concerne la protection des données. Nous pouvons en tirer des conseils qui sont valables de manière générale pour les fournisseurs.

Quant aux utilisateurs, ils peuvent également veiller à améliorer la protection des données: en choisissant délibérément dans la pléthore de produits disponibles ceux qui répondent le mieux à leurs exigences.

Conseils pour les utilisateurs

- **Choisir une solution avec fonction de cryptage (si possible basée sur un standard ouvert):** Comme chacun sait, Internet est un réseau public qui n'est a priori pas en mesure de garantir la confidentialité des données. Cela signifie que les conversations non cryptées pourraient être interceptées par des personnes non autorisées. Ceci vaut surtout lors de l'utilisation d'un réseau sans fil (WLAN) non protégé. Comme les conversations téléphoniques peuvent contenir des données personnelles sensibles, il est fortement conseillé d'utiliser le cryptage. L'usage d'un système de cryptage requiert toujours une certaine confiance de la part de l'utilisateur. C'est pourquoi la préférence doit être donnée à une solution basée sur un standard ouvert (donc vérifiable) plutôt qu'à une solution propriétaire.

- **Installer régulièrement les mises à jour du logiciel:** Tout logiciel révèle au cours du temps des erreurs ou des failles de sécurité. C'est pourquoi les éditeurs de logiciels sérieux fournissent régulièrement des mises à jour correctives pour leurs produits. Nous conseillons donc à tout utilisateur de s'assurer qu'il utilise toujours la version la plus récente d'un logiciel VoIP.

- **Activer les options de confidentialité en fonction des besoins personnels:** Les options de confidentialité des données ne présentent un avantage que si l'utilisateur les active en fonction de ses besoins. Ainsi, la suppression de l'affichage du numéro appelant (identité) peut présenter un avantage pour l'appelant lors de certains appels, et un inconvénient pour d'autres. Il n'est donc pas indiqué de conseiller que toutes les options de confidentialité soient toujours activées.

Conseils pour les éditeurs de logiciel

- **Proposer un cryptage:** La confidentialité des conversations ne peut être assurée que si les flux de données sont cryptés. C'est la raison pour laquelle un éditeur devrait absolument proposer une fonction de cryptage.

- **Utiliser des standards ouverts:** Pour des raisons de confiance et de transparence, la préférence doit être donnée à des standards ouverts. Ceci vaut surtout pour le cryptage. Ainsi, l'utilisation d'un protocole de communication ouvert donne la possibilité à des tiers d'offrir des produits de sécurisation (par ex. Zfone).

- **Rendre l'installation et l'utilisation faciles:** L'expérience montre qu'un produit n'est adopté par un grand nombre d'utilisateurs que s'il peut être installé, configuré et utilisé facilement et sans nécessiter des connaissances spéciales ou expériences préalables.

- **Informer sur les risques en matière de protection et de sécurité des données:** Les éditeurs doivent informer les utilisateurs en détail sur les traitements de données qui sont effectués lorsque ceux-ci utilisent leur produit (clause de confidentialité). Ceci inclut également les éventuels risques pour la protection et la sécurité des données. Ce n'est que s'ils possèdent ces informations que les utilisateurs peuvent efficacement se protéger.

- **Réduire au minimum les traitements de données:** Conformément aux principes de minimisation et/ou d'évitement de données, on ne traitera que les données qui sont absolument nécessaires pour assurer la prestation de service.

- **Corriger rapidement les erreurs identifiées et proposer des mises à jour automatiques:** Les erreurs identifiées qui ont une incidence sur la protection ou la sécurité des données doivent être immédiatement corrigées. Les utilisateurs doivent être informés rapidement et de manière bien visible que des mises à jour sont disponibles.

- **Inclure des options de sécurisation qui sont activées par défaut:** L'expérience montre que les utilisateurs n'explorent pas activement les options qu'offre un logiciel. C'est pourquoi il est conseillé de prérégler les options de sécurisation et de protection des données. Ainsi, l'utilisateur devrait par exemple pouvoir choisir au moment de l'installation s'il désire figurer dans l'«annuaire électronique» ou non.

4.3 Recommandation concernant le traitement et la communication de données électroniques par la société X sur mandat de détenteurs de droits d'auteur.

Voir paragraphe 4.3 de la partie en langue allemande.

4.4 Recommandation concernant les tests de dépistage de drogues et d'alcool auprès des CFF

Voir paragraphe 4.4 de la partie en langue allemande.

4.5 Recommandation concernant le traitement de données extraites du registre du commerce par la société X

Voir paragraphe 4.5 de la partie en langue allemande.

4.6 Recommandation adressée à l'Office fédéral de la santé publique: «Contrat vaccin pré-pandémique I»

Voir paragraphe 4.6 de la partie en langue allemande.

4.7 Recommandation adressée à l'Office fédéral des transports: «Tableaux de service des entreprises de chemins de fer»

Voir paragraphe 4.7 de la partie en langue allemande.

4.8 Recommandation adressée au Département fédéral des affaires étrangères: «Procès-verbal de la 5ième séance du comité mixte sur la libre circulation des personnes UE»

Voir paragraphe 4.8 de la partie en langue allemande.

4.9 Recommandation adressée à l'Office fédéral des assurances privées: «calculs de tarifs»

Voir paragraphe 4.9 de la partie en langue allemande.

4.10 Recommandation adressée à l'Office fédéral des migrations: «Liste des critères des «Safe countries» (pays considérés comme sûrs)»

Voir paragraphe 4.10 de la partie en langue allemande.

4.11 Recommandation adressée à l'EPFZ: «Acides gras trans»

Voir paragraphe 4.11 de la partie en langue allemande.

4.12 Recommandation adressée à La Poste Suisse: «PostFinance»

Voir paragraphe 4.12 de la partie en langue allemande.

4.13 Recommandation adressée à Swissmedic: «Demande d'autorisation de mise sur le marché de médicaments»

Voir paragraphe 4.13 de la partie en langue allemande.

4.14 Recommandation adressée à l'Office fédéral de l'environnement «Projet d'ordonnance de la protection contre les vibrations»

Berne, le 18 décembre 2007

Recommandation

émise au titre

de l'art. 14
de la loi fédérale du 17 décembre 2004
sur le principe de la transparence
dans l'administration

relativement à la demande en médiation introduite

par les opposants au projet CEVA à Genève,
représentés par
X

contre

l'Office fédéral de l'environnement, Berne

I. Le préposé fédéral à la protection des données et à la transparence constate ce qui suit:

1. Le demandeur, avocat, mandaté par plusieurs opposants au projet CEVA[1] à Genève, a déposé le 27 février 2007 auprès de l'Office fédéral de l'environnement (OFEV) une demande d'accès au «projet d'ordonnance sur la protection contre les vibrations qui est en cours d'examen par votre office».

2. Le 9 mars 2007, l'OFEV a répondu au demandeur: «La consultation des offices n'est actuellement pas terminée. Tant qu'une unité n'a pas été trouvée, le document que vous demandez reste confidentiel.» L'OFEV a en outre prié le demandeur de patienter jusqu'à l'ouverture de la consultation officielle (au sens de la loi fédérale sur la procédure de consultation, RS 172.061), «qui selon les informations à disposition aujourd'hui devrait avoir lieu début 2008.»

3. Le 19 mars 2007, le demandeur a requis une décision de l'OFEV. Le 12 avril 2007, l'OFEV a répondu qu'aucun accès n'allait être accordé, conformément aux art. 7, al. 1, let. a, et 8, al. 2, de la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans; RS 152.3). Ayant omis, par inadvertance, de faire savoir dans sa lettre du 9 mars 2007 au demandeur que ce dernier pouvait introduire une demande en médiation auprès du préposé fédéral à la protection des données et à la transparence (préposé), l'OFEV a directement informé le préposé, en le priant d'ouvrir une procédure de médiation.

4. Dans le cadre de cette procédure, l'OFEV a remis au préposé un avis sur la question ainsi que de nombreux documents relatifs au projet d'ordonnance sur la protection contre les vibrations.

II. Le préposé fédéral à la protection des données et à la transparence prend en considération les éléments suivants:

A. Médiation selon l'art. 14 LTrans

1. En vertu de l'art. 13 LTrans, toute personne peut déposer une demande en médiation lorsque sa demande d'accès à des documents officiels est limitée, différée ou refusée, ou lorsque l'autorité n'a pas pris position sur sa demande dans les délais.

[1] Liaison ferroviaire Cornavin – Eaux-Vives – Annemasse (CEVA)

Le préposé n'agit pas d'office, mais seulement sur la base d'une demande déposée par écrit[2]. Est habilitée à introduire une demande en médiation toute personne qui a pris part à une procédure de demande d'accès à des documents officiels. Pour la présentation de la demande en médiation, la forme écrite simple suffit. La demande doit spécifier que l'affaire est confiée au préposé. Elle doit être remise dans les 20 jours qui suivent la réception de la prise de position de l'autorité.

2. Le demandeur a déposé une demande d'accès au sens de l'art. 6 LTrans auprès de l'OFEV et en a reçu une réponse négative. Ayant ainsi participé à une procédure de demande d'accès antérieure, il est qualifié pour déposer une demande en médiation.

3. La procédure de médiation peut se dérouler par écrit ou de vive voix (en présence de tous les intéressés ou de certains d'entre eux), sous l'égide du préposé. C'est à lui qu'il incombe de fixer les modalités[3].

   Si la médiation n'aboutit pas ou si aucune solution consensuelle n'est envisageable, le préposé est tenu par l'art. 14 LTrans de formuler une recommandation fondée sur son appréciation de l'affaire.

B. Champ d'application matériel

1. Le demandeur a requis l'accès à l'état le plus récent d'un projet d'ordonnance auquel travaille l'OFEV. L'OFEV a fait savoir au demandeur que ce projet, après avoir fait l'objet d'une première consultation des offices[4], en était au stade de l'élimination des divergences. Il a donc refusé l'accès au projet d'ordonnance en s'appuyant sur les art. 7, al. 1, let. a, et 8, al. 2, LTrans.

2. L'art. 8 LTrans porte que l'accès aux documents officiels n'est autorisé qu'après la décision politique ou administrative dont ils constituent la base. Le projet que le Conseil fédéral avait soumis au Parlement n'allait pas aussi loin et portait explicitement que le droit d'accès aux documents officiels afférents à la *procédure de consultation des offices* n'existait qu'après la décision du Conseil fédéral (art. 8, al. 1, let b, du projet LTrans). Cette solution devait garantir à l'exécutif qu'il pouvait «former librement son opinion et sa volonté»[5]. Lors des

[2] FF 2003 1864
[3] FF 2003 1865
[4] Cf. art. 4 de l'ordonnance sur l'organisation du gouvernement et de l'administration (OLOGA, RS 172.010.1)
[5] FF 2003 1856

débats parlementaires[6], la teneur de cette disposition a été modifiée en ce sens que, d'une part, l'accès à tous les documents officiels (et non aux seuls documents afférents à la procédure de consultation des offices) n'est autorisé qu'après la décision politique ou administrative dont ils constituent la base. D'autre part, cette disposition ne concerne plus seulement le Conseil fédéral, mais *toutes les autorités*.

3. En principe, un office fédéral peut restreindre l'accès à tous les documents susceptibles de constituer la base d'une décision non encore arrêtée. Le préposé est toutefois d'avis qu'un document ne peut être soustrait au droit d'accès que s'il présente effectivement un *lien temporel et matériel* avec une décision pendante. Il n'est donc pas admissible qu'une autorité retienne un document sous prétexte qu'il pourrait *éventuellement* constituer à l'avenir une base pour une décision fondamentale. Bien plutôt, l'autorité doit pouvoir attester qu'une décision sera prise dans un délai prévisible ou que le dossier en cause fait encore l'objet d'une élaboration en vue d'une décision à prendre.

   Dans le cas du projet d'ordonnance qui nous occupe ici, la première consultation des offices a eu lieu durant l'été 2006. L'OFEV a pu montrer de façon probante au préposé que les travaux engagés par l'office et par le département allaient, selon toute probabilité, déboucher sur une décision à brève échéance, à savoir sur une consultation publique durant le premier semestre de l'année 2008.

   Le préposé en arrive donc à la conclusion que l'OFEV a agi conformément à la loi sur la transparence lorsqu'il a différé l'accès au dernier état du projet d'ordonnance sur la protection contre les vibrations.

4. La question de savoir si l'exception prévue à l'art. 7, al. 1, let. a, LTrans s'appliquera ou non ne pourra trouver de réponse que lorsque la décision politique ou administrative visée à l'art. 8, al. 2, LTrans aura été prise: le droit d'accès est différé jusque-là. Par la suite, le document officiel sera en principe accessible. Il est toutefois possible qu'une autorité puisse alors en limiter l'accès en vertu d'une des exceptions prévues à l'art. 7 LTrans.

[6] Bulletin officiel — Conseil national BO 2004 N 1258ss (proposition de minorité relative à l'art. 4); Bulletin officiel — Conseil des États BO 2004 E 592s. (transformation de l'art. 4 en art. 8 pour une raison de systématique)

III. Se fondant sur les considérations ci-dessus, le préposé fédéral à la protection des données et à la transparence recommande ce qui suit:

1. L'Office fédéral de l'environnement maintient l'ajournement de l'accès au projet d'ordonnance sur la protection contre les vibrations. Il informera le demandeur aussitôt qu'une décision politique ou administrative au sens de l'art. 8, al. 2, LTrans aura été prise et accordera l'accès au document officiel correspondant.

2. Dans les dix jours qui suivent la réception de la recommandation, le demandeur peut demander que l'Office fédéral de l'environnement rende une décision selon l'art. 5 de la loi fédérale sur la procédure administrative (art. 15, al. 1, LTrans).

3. Par analogie à l'art. 22a de la loi fédérale sur la procédure administrative (RS 172.021), les délais fixés en jours par la loi ne courent pas du 18 décembre au 2 janvier. Le délai débute donc le 3 janvier 2008.

4. La décision peut faire l'objet d'un recours devant le Tribunal administratif fédéral (art. 16, LTrans).

5. La présente recommandation est publiée (art. 13, al. 3, de l'ordonnance sur la transparence, OTrans; RS 152.31). Afin de protéger les données relatives aux parties à la procédure de médiation, le nom du demandeur a été anonymisé.

6. La recommandation est notifiée à:

   - X
   - l'Office fédéral de l'environnement
     003 Berne

Hanspeter Thür

4.15 Recommandation adressée à l'Office fédéral de la communication: «Rapport sur la qualité du service universel de Swisscom Fixnet SA»

Voir paragraphe 4.15 de la partie en langue allemande.

4.16 Recommandation adressée à l'Office fédéral de la santé publique: «Contrat vaccin pré-pandémique II»

Voir paragraphe 4.16 de la partie en langue allemande.

4.17 Recommandation adressée à l'Office fédéral de l'environnement: «Liste des adresses et déclarations de taxe des détenteurs de décharge et des exportateurs des déchets»

Voir paragraphe 4.17 de la partie en langue allemande.

4.18 Declaration adopted by the European Data Protection Authorities in Cyprus on 11 May 2007

Voir paragraphe 4.18 de la partie en langue allemande.

4.19 Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement

Voir paragraphe 4.19 de la partie en langue allemande.