14ème Rapport d'activités 2006/2007

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2006/2007 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 2006 au 31 mars 2007.

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. 410.014.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Par trop souvent, le préposé à la protection des données se retrouve dans le personnage de Sisyphe, cette figure tragique de la mythologie grecque condamnée à remonter une pente en poussant un énorme rocher qui, aussitôt arrivé en haut, retombe inéluctablement: à peine croit-on avoir résolu un problème de protection des données qu'il réapparaît sous une forme légèrement différente. Tel a été le cas, après bien des discussions entre le PFPDT et le Conseil fédéral, au sujet de l'absence de bases légales lors de l'engagement de drones de reconnaissance en faveur du Corps des gardes-frontière. Suite à diverses motions parlementaires, le Conseil fédéral semble désormais être revenu sur sa position initiale de refus et prêt à combler cette lacune par une révision partielle de la législation militaire. Mais le sujet ne va pas cesser de nous préoccuper: des avions miniatures télécommandés ou même programmés par GPS (hélicoptères, drones, etc.), équipés d'appareils de prise de vue à haute résolution, apparaissent sur le marché, à toutes sortes de fins plus ou moins légales, et de plus en plus de citoyennes et de citoyens s'en inquiètent. En matière de protection de la sphère privée, cette évolution vers une miniaturisation de la technologie au service de la surveillance sera un grand défi de l'avenir. De concert avec d'autres organes concernés, nous nous consacrerons à la question avec la fermeté qui s'impose.

La surveillance croissante, dans ses manifestations les plus diverses, demeure un sujet de préoccupation constante. Au niveau national bien sûr, où la révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) entre dans la phase délicate des délibérations parlementaires: cette modification vise une extension radicale des possibilités d'intervention des organes de la protection de l'Etat dans la sphère privée des particuliers. Mais au niveau international également, la liberté personnelle voit sa marge de plus en plus rétrécie. Avec nos homologues européens, nous nous attacherons à suivre l'évolution de l'Europe vers une collaboration policière et judiciaire renforcée dans les affaires pénales et mettrons tout en œuvre pour garantir un haut niveau de protection des données.

Nous classerons au même chapitre la transmission d'informations aux autorités américaines par la centrale de la SWIFT à Bruxelles dans le cadre de la lutte anti-terroriste. Ce sujet nous a grandement préoccupés au cours de l'année écoulée (voir chiffre 1.8.1). Nous avons surtout critiqué le fait qu'à partir de la Suisse, des prestataires financiers ont livré des données concernant des clients à la SWIFT, qui se trouve en Belgique, sans en informer ces mêmes clients. Malheureusement, jusqu'à ce jour, tous les instituts bancaires suisses ne se sont pas conformés au devoir de transparence que nous avons requis. La Suisse se doit aussi d'agir en vue d'un accord visant à im-

poser des règles de protection des données à la livraison, aux Etats-Unis, de ce genre de données (nul n'ignore en effet que les Etats-Unis ne disposent toujours pas de dispositions en matière de protection des données comparables à celles de la Suisse). A ce propos, l'action doit se situer au niveau politique. Comme nous l'avons appris fin mars 2007, il est à saluer que la société SWIFT elle-même ait accepté, sous la pression des autorités belges de protection des données, de se soumettre aux règles fondées sur le système dit du Safe Harbour. Il est permis de douter qu'une protection suffisante soit ainsi garantie et qu'une action au niveau suisse s'en trouve superflue. Nous suivrons cette évolution avec attention. Dans ce contexte, il est intéressant de noter que souvent, des questions déjà délicates touchant la protection des données peuvent faire émerger d'autres problèmes particulièrement graves: en mars 2007, la SWIFT a été attaquée par des banques allemandes qui craignaient que des informations concernant des transactions financières européennes soient exploitées abusivement par les services secrets américains à des fins d'espionnage économique. Un exemple frappant de l'importance majeure que la protection des données devrait revêtir pour l'économie.

La santé demeure un grand chantier qui continue à absorber beaucoup d'énergie. Les sujets de préoccupation vont de la carte de santé à l'introduction de l'électronique dans les services de médecins-conseils, en passant par la carte d'assuré, le dossier électronique des patients et les DRG, pour ne mentionner que les plus importants. A l'ère du tout électronique, et justement dans le domaine de la santé où les données traitées sont très sensibles, des accidents majeurs en matière de protection des données sont à craindre. En effet, du fait de ses moyens en la matière, le PFPDT ne peut intervenir que sporadiquement ou lorsqu'une violation des règles de protection des données a déjà eu lieu. Ensuite, il doit se contenter de transmettre des recommandations. L'Office fédéral de la santé (OFSP) doit ici assumer sa responsabilité en tant qu'autorité de surveillance avec droit de donner des instructions.

Avec l'entrée de la loi sur la transparence le 1er juillet de l'année dernière, une nouvelle tâche nous a été attribuée. Trois procédures de médiation (médiation prévue par la loi entre les citoyens et l'administration en cas de litige) ont été menées durant les six premiers mois. Comme nous l'avions annoncé, nous avons dû mener ces procédures de manière extrêmement serrée. Dans ces conditions, on ne peut guère parler de véritable médiation. Malgré cela, ces procédures ont été extrêmement longues et laborieuses, en raison du volume des dossiers et de la complexité des problèmes, jusqu'à ce que nous puissions remettre une recommandation fondée. En tout état de cause, une telle recommandation, si elle n'est pas acceptée par les parties, devra éventuellement résister aux critiques des autorités judiciaires dans le cadre d'une procédure de

recours. Au cours des trois premiers mois de l'année 2007, nous avons déjà reçu treize autres demandes. Jusqu'à ce jour, le Conseil fédéral a maintenu sa décision de ne pas accorder les postes supplémentaires envisagés à l'origine pour cette tâche. Les travaux effectués jusqu'ici, qui devraient encore considérablement augmenter au cours de l'année qui vient, n'ont pu être menés à bien que parce que la Chancelière fédérale a mis à notre disposition un poste limité dans le temps financé sur son propre budget du personnel. Malgré cette mesure, il est toutefois à craindre que les demandes en suspens ne pourront pas être traitées dans le délai prévu par la loi.

L'année dernière déjà, j'avais fait état de mes préoccupations au sujet de notre budget du personnel, extrêmement modeste en comparaison internationale et toujours plus sous pression du fait des mesures d'économie et de l'augmentation des tâches. Etant donné qu'au niveau politique, aucun indice de changement fondamental ne semblait se dessiner dans un avenir plus ou moins rapproché, nous avons décidé d'examiner, dans le cadre d'un plan rigoureux d'abandon des tâches, comment malgré tout remplir encore de manière crédible notre mandat légal avec les moyens dont nous disposons. Nous avons donc pris le parti, à l'avenir, de nous consacrer uniquement aux questions de protection des données ayant une grande portée pour la sphère privée d'un grand nombre de personnes. Concrètement, cela signifie que nous ne répondrons plus individuellement aux questions émanant de particuliers. Nous tenons toutefois à demeurer à leur écoute et avons mis sur pied un service de renseignements téléphoniques tous les jours de 10 à 12 heures. En outre, des réclamations peuvent nous être transmises par écrit ou par courriel. Nous les traiterons en fonction de leur importance et de nos moyens. Par ailleurs, nous avons aménagé notre site web dans l'optique de créer une plateforme d'informations et espérons ainsi offrir une solution de rechange un tant soit peu acceptable aux quelque 1500 particuliers qui, année après année, s'adressent directement à nous.

Hanspeter Thür

Répertoire des abréviations

ASSM	Académie Suisse des Sciences Médicales
CEDH	Convention européenne de sauvegarde des droits de l'homme et de ses libertés fondamentales
CFMJ	Commission fédérale des maisons de jeu
CFPDT	Commission fédérale de la protection des données et de la transparence
CNIL	Commission nationale de l'informatique et des libertés
CP	Code pénal
Cst.	Constitution fédérale
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
DRG	Diagnosis Related Group
fedpol	Office fédéral de la police
GEWA	Système de traitement de données en matière de lutte contre le blanchiment d'argent
HOOGAN	Système d'information pour la lutte contre le hooliganisme
IPAS	Système informatisé de gestion et d'indexation de dossiers et de personnes
ISIS	Système de traitement de données relatives à la protection de l'Etat
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAA	Loi fédérale sur l'assurance-accidents
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants

LBA	Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier
LCD	Loi fédérale contre la concurrence déloyale
LHR	Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes
LMJ	Loi fédérale sur les maisons de jeu
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
LPD	Loi fédérale sur la protection des données
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
LRH	Loi fédérale relative à la recherche sur l'être humain
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
OALSP	Ordonnance concernant les autorisations de lever le secret professionnel en matière de recherche médicale
OCPD	Ordonnance de certification en matière de protection des données
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFSP	Office fédéral de la santé publique
OFSPO	Office fédéral du sport
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

PFPDT	Préposé fédéral à la protection des données et à la transparence
PJF	Police judiciaire fédérale
RIPOL	Système de recherches informatisées de police
SAP	Service d'analyse et de prévention
SECO	Secrétariat d'Etat à l'économie
SIS	Système d'information de Schengen
SYMIC	Système d'information central sur la migration
TF	Tribunal fédéral
TFA	Tribunal fédéral des assurances
USIC	Unité de stratégie informatique de la Confédération
VOSTRA	Casier judiciaire informatisé

1 Protection des données

1.1 Droits fondamentaux

1.1.1 Projet d'ordonnance de certification en matière de protection des données

En raison de leur portée, de leur étendue et de leur relative complexité, les exigences de certification ont été regroupées au sein d'une ordonnance spécifique (OCPD). La certification d'organisations s'inspire fortement de la norme ISO 27001 pour son système de gestion de protection des données, tandis que la certification de produits se base sur le catalogue d'exigences pour l'expertise de produits-IT en vigueur depuis quelques années dans le Land allemand du Schleswig-Holstein.

Dans le cadre de mise en application du nouvel article 11 de la LPD adopté en mars 2006 par l'Assemblée fédérale, nous avons poursuivi notre collaboration avec l'Office fédéral de la justice et le Service d'accréditation suisse, dans le but de définir les conditions et exigences minimales relatives à l'obtention d'une certification de protection des données. L'idée d'élaborer une ordonnance spécifique pour la certification (OCPD) s'est assez rapidement imposée, en raison des nombreuses exigences particulières relatives tant aux organisations/procédures qu'aux produits/systèmes. Les premiers articles de l'OCPD définissent les conditions générales d'obtention, d'utilisation, de validité et de reconnaissance de ces certifications en matière de protection des données, ainsi que les rôles respectifs des différents partenaires concernés. Pour rappel, on part du principe qu'avec un niveau de protection des données reconnu conforme au moment de l'audit et une gestion active et documentée de l'évolution, une certification de protection des données peut être délivrée pour une période de quelques années (voir ch.1.1.1 de notre 13ème rapport d'activités 2005/2006).

Pour la certification d'organisations, nous avons soumis notre projet de référentiel-type à un groupe de travail formé de plusieurs entreprises suisses de certification d'organisations selon les systèmes de gestion ISO 9001:2000 (qualité) et 27001:2005 (sécurité de l'information). L'annexe 1 de l'OCPD adapte et étend les exigences d'ISO 27001 à celles découlant de la LPD, ce qui en fait un véritable catalogue d'exigences pour les systèmes de gestion de la protection des données (SGPD). Le chapitre 3 comprend en particulier les dix principes ou exigences de protection des données suivants: licéité – transparence – proportionnalité – finalité – exactitude - communication à l'étranger - sécurité des données - traitement par des tiers - liste des fichiers - droit d'accès.

A l'instar de la certification ISO 27001 qui se base intégralement sur le code de pratique ISO 17799:2005 pour la gestion de la sécurité de l'information (11 groupes, 39 objectifs et 133 mesures), nous allons publier et actualiser un code de pratique complémentaire pour la gestion et la certification de protection des données. Celui-ci sera dédié exclusivement à la protection des données et à la confidentialité des informations relatives à la vie privée (mesure générique originelle 15.1.4 de la norme 17799:2005) et permettra la mise en oeuvre des dix objectifs de protection des données précités, grâce à une vingtaine de mesures spécifiques, fidèlement structurées selon les recommandations ISO. Pour la certification de produits, notre choix s'est porté - faute de normes internationales véritablement adaptées et reconnues - sur le catalogue d'exigences pour l'expertise de produits-IT dans le cadre du procédé de certification en vigueur au Schleswig-Holstein. La structuration des exigences en quatre couches logiques distinctes (conception technique – conformité - mesures techniques et organisationnelles - droits de la personne concernée) nous a particulièrement convaincus, de même que le fait de prévoir un profil séparé pour les données accessoires (logdata). Ces dernières constituent en effet des fichiers annexes dont les finalités et conditions de traitement sont en principe différentes de celles du fichier principal. L'annexe 2 de l'OCPD contiendra ainsi une adaptation au droit suisse de ce catalogue d'exigences qui a déjà fait ses preuves en Allemagne septentrionale.

Enfin, l'OCPD comprendra une annexe 3 consacrée aux exigences pour la qualification du personnel des entreprises certificatrices, ainsi qu'une annexe 4 recensant les sigles de qualité proposés par la Confédération pour la certification complète ou partielle d'organisations et pour la certification de produits. L'usage et la reconnaissance de sigles privés sont également réglés par l'ordonnance. La procédure de consultation externe relative à l'ordonnance d'application et à l'ordonnance de certification a été ouverte fin février 2007 par l'OFJ. A notre surprise et regret nous avons appris juste avant l'expiration du délai de rédaction du présent rapport que les annexes 1, 2 et 4 - prévues de longue date – avaient été supprimés.

1.1.2 L'harmonisation des registres officiels de personnes et l'utilisation du nouveau numéro d'assuré AVS comme identificateur de personnes

Le nouveau numéro d'assuré AVS sera utilisé comme numéro d'assurance sociale et comme identificateur administratif de personnes dans les registres harmonisés. Ainsi en a décidé le Parlement. Les cantons prévoient également d'utiliser ce numéro de manière systématique.

L'Office fédéral de la statistique (OFS) a déjà élaboré plusieurs projets relatifs à l'identificateur de personnes, projets qui ont chaque fois été soumis à des consultations (cf. notre 13ème rapport d'activités 2003/2004, ch. 1.2.1). Le Parlement a maintenant statué: la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (LHR) ainsi que la révision de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) prévoient que le nouveau numéro d'assuré AVS soit utilisé d'une part comme numéro d'assurance sociale, d'autre part comme numéro d'identification personnelle à des fins administratives. Les lois ont été adoptées le 23 juin 2006.

Dans le cadre de consultations des offices ainsi que lors de séances du Parlement relatives aux projets de loi, nous avons pris position et proposé une solution alternative. Notre démarche était guidée par les réflexions suivantes:

Le fait de mêler les exigences de la statistique à celles de l'administration est très problématique du point de vue de la protection de la personnalité. La statistique a besoin de données pseudonymisées en provenance d'un nombre aussi élevé de sources que possible alors que l'administration requiert des données personnelles aussi précises que possible. L'introduction d'un numéro d'identification de personnes (sous la forme du nouveau numéro d'assuré AVS) facilite la mise en relation de données personnelles provenant de divers registres. Avec une telle mise en relation, les personnes concernées ne seraient plus en mesure de savoir quels traitements sont effectivement effectués avec leurs données.

Le modèle autrichien (décrit sur le site http://www.cio.gv.at/egovernment/umbrella/) utilise des identificateurs de personne spécifiques à des domaines, tout en étant tous dérivés d'un même numéro de base crypté. Un tel modèle présenterait des avantages indubitables pour une future cyberadministration suisse. C'est pourquoi nous sommes d'avis qu'il faut une infrastructure technique qui permette de séparer clairement les besoins de la statistique et de l'administration et qui garantisse en même temps qu'un

transfert de données non prévu puisse être exclu au niveau technique. Nous avons présenté et expliqué le modèle autrichien aux parlementaires alors qu'ils travaillaient sur la LHR et la LAVS ; malheureusement cette solution n'a pas été retenue pour la Suisse.

Les lois ayant été adoptées, il s'agit maintenant d'élaborer les dispositions d'exécution et de mettre en œuvre l'harmonisation des registres dans les cantons. Dans ce contexte, le canton de Berne a joué un rôle de précurseur: le Grand Conseil a adopté la loi sur l'harmonisation des registres officiels (LReg) le 28 novembre. A l'article 9, cette loi prévoit l'utilisation systématique du numéro d'assuré AVS selon la LAVS.

Alors que d'autres cantons ont également déjà présenté ou vont présenter des projets de loi pour une harmonisation des registres, nous avons publié – en collaboration avec «privatim – les commissaires suisses à la protection des données» – une prise de position sur l'utilisation par les cantons du numéro d'assuré AVS. Dans l'optique de la protection des données, l'utilisation par les cantons du numéro d'assuré AVS comme identificateur général de personnes doit être légitimée par un travail législatif soigné. Une loi autorisant l'utilisation générale du numéro d'assuré AVS pour toutes les tâches administratives cantonales serait en effet inadmissible. L'extension du champ d'application de ce numéro d'assuré pour en faire un numéro universel présente des risques importants pour la sphère privée des citoyens et des citoyennes, en raison des connexions indésirables que cette extension permet d'établir entre différentes bases de données. L'Office fédéral des assurances sociales s'est aussi prononcé dans ce sens. En décembre 2002 déjà, nous avions demandé au Professeur Biaggini une expertise sur le thème «Un identificateur de personne sous l'angle de la protection de la personnalité prévue dans le droit constitutionnel (art. 13 Cst.)». Le rapport d'expertise (uniquement en allemand) ainsi que les prises de position peuvent être consultés à l'adresse:

http://www.edoeb.admin.ch/themen/00794/00819/01081/index.html?lang=fr).

1.1.3 Communication d'informations au public par un office fédéral

Un office fédéral a le droit, même sans le consentement de la personne concernée, de communiquer des données personnelles dans le cadre de l'information officielle du public. Encore faut-il que ces informations soient en rapport avec l'accomplissement de tâches publiques et que la communication réponde à un intérêt public prépondérant. Il convient dans chaque cas d'espèce de veiller au respect des principes généraux de la protection des données, en particulier au respect du principe de la proportionnalité.

Un office fédéral nous a demandé si la législation sur la protection des données lui permettait de rectifier des informations erronées relayées par la presse au sujet d'un dossier individuel, en communiquant certains éléments du dossier afin d'informer le public sur la réalité des faits.

La rectification, par un organe fédéral, d'informations erronées fournies et relayées par des médias constitue, dans la mesure où ces informations se rapportent à une personne identifiée ou identifiable, une communication de données personnelles au sens de l'art. 19 LPD et doit en respecter le cadre légal.

Selon l'art. 19 LPD, les organes fédéraux ne peuvent communiquer des données personnelles que s'il existe une base légale ou dans des cas bien particuliers, expressément prévus par la LPD, notamment lorsque la personne concernée a donné son consentement ou qu'elle a rendu ses données accessibles à tout un chacun. Depuis le 1er juillet 2006, le cadre juridique de l'art. 19 LPD a été élargi et désormais, les organes fédéraux peuvent communiquer des données personnelles dans le cadre de l'information officielle du public, d'office ou en vertu de la loi sur la transparence, à condition que les données concernées soient en rapport avec l'accomplissement de tâches publiques et que la communication réponde à un intérêt public prépondérant.

Il convient, dans chaque cas d'espèce, d'apprécier si et dans quelle mesure la communication de données personnelles dans le cadre de l'information officielle du public est justifiée. Il faut notamment veiller au respect des principes généraux de la protection des données, en particulier au respect du principe de la proportionnalité: par exemple, les données personnelles doivent dans la mesure du possible être rendues anonymes; seules les données personnelles qui sont absolument nécessaires pour informer le public peuvent être communiquées.

1.1.4 Vote électronique: impression sur papier des votes électroniques (paper trail)

Un point délicat dans le contexte du vote électronique est l'exigence de pouvoir retracer les suffrages. Nous avons discuté de ce problème avec les organes fédéraux impliqués. Il est maintenant prévu d'en débattre dans le groupe de travail «Vote électronique».

Depuis plusieurs années, la Chancellerie fédérale mène des projets pilotes en matière de vote électronique avec les cantons de Genève, de Neuchâtel et de Zurich. En mai 2006, elle a soumis au Conseil fédéral un rapport à l'intention du Parlement présentant un bilan de ces projets pilotes. Ce bilan est en principe positif et prône une extension du vote électronique. Un des points délicats qui y est mentionné est le problème de la traçabilité des votes et l'exigence d'une impression sur papier des votes électroniques (Paper Trail; cf. aussi notre 9ème rapport d'activités 2001/2002, ch. 1.1). La Chancellerie fédérale a invité des représentants du PFPDT et de l'Unité de stratégie informatique de la Confédération (USIC) à une séance afin de discuter des questions du secret du vote, de la protection des données et de la sécurité informatique ainsi que de l'exigence d'un «paper trail».

La procédure détaillée pour traiter le problème du «paper trail» et de la traçabilité sera discutée dans le groupe de travail «Vote électronique».

1.1.5 E-Government et protection des données

Nous avons été invités à apporter notre contribution dans le cadre d'une journée organisée à Bellinzone sur le thème du E-Governement. La journée faisait partie de la manifestation «Tecnologia e Diritto» (Technologie et droit), organisée chaque année par l'Ecole supérieure d'informatique de gestion de Bellinzone.

Le E-Government est un objectif stratégique de la Confédération. Il représente un cas typique de matière multidisciplinaire, qui touche tant le droit que l'informatique et qui pose des défis à la protection des données.

Les projets du E-Government pourraient, en théorie, couvrir toutes les transactions entre les autorités (fédérales, cantonales et communales) et les citoyens; ils ont pour but d'améliorer et optimiser les différents services. Un exemple classique est l'annonce de changement de domicile; cette opération pourrait être accomplie sur Internet, ce qui éviterait de passer physiquement aux différentes chancelleries communales. Ce genre de projets ne comporte pas seulement des avantages, mais aussi des risques du point de vue de la protection des données (dans le cas cité, il faudra par exemple éviter que les données en question soient interceptées par des tiers non autorisés).

Pour améliorer et compléter la discussion et la compréhension du domaine, l'Ecole supérieure d'informatique de gestion de Bellinzone a décidé de dédier l'édition 2006 de la manifestation «Tecnologia e Diritto» (Technologie et droit) au thème du E-Government et a choisi d'inviter une délégation du PFPDT dans le but de présenter les risques pour la protection des données dans ce domaine. Nous en avons profité pour présenter également les développements récents concernant l'introduction d'un numéro personnel unique (cf. ch. 1.1.2), ainsi que la solution autrichienne (cf. 13ème rapport d'activités 2005/2006, ch. 1.2.1)

1.1.6 La publication d'arrêts du Tribunal fédéral sur Internet

Les arrêts du Tribunal fédéral à partir de l'année 1954 (et, depuis leur fusion, également ceux du Tribunal fédéral des assurances) ont été publiés sur Internet. Les jugements n'ont pas tous été anonymisés et peuvent contenir des données personnelles sensibles. Nous conseillons dans de tels cas de demander une anonymisation de la publication sur Internet.

Nous avons déjà abordé la problématique de la publication des arrêts du Tribunal fédéral du point de vue de la protection des données dans notre 9ème rapport d'activités 2001/2002 (au ch. 2.3.3). Il s'agissait à l'époque des jugements qui avaient été publiés sur la toile à partir de l'année 2000.

Nous désirons aborder ici un autre aspect, à savoir celui des jugements plus anciens qui ont été rendus à une époque où personne ne pensait à une publication ultérieure sous forme électronique. Entre-temps, de tels jugements du Tribunal fédéral (TF) et du Tribunal fédéral des assurances (TFA) ont également été publiés sur Internet (www.bger.ch).

Une personne a constaté qu'une recherche effectuée dans les moteurs de recherche d'Internet avec son nom et prénom aboutissait sur le texte intégral d'un arrêt du TFA datant des années 1980. Cet arrêt contenait des données très sensibles, notamment sur l'état de santé de la personne concernée. L'arrêt avait à l'époque été publié sous forme papier et était donc publiquement accessible. Une publication accessible de nos jours sur Internet doit cependant être vue sous un angle nouveau: une recherche permet de la retrouver très facilement et très rapidement depuis n'importe où dans le monde.

La personne concernée s'est adressée au tribunal et a demandé que l'arrêt en question soit anonymisé. Heureusement, ce dernier a donné suite à sa demande. Il est important de noter qu'un arrêt du TF ou du TFA, dont la version officielle publiée sur Internet a été anonymisée, ne disparaît pas forcément de la toile, car il existe d'autres organisations qui publient des jugements et les gèrent dans leur propre base de données. Cela signifie qu'il faudrait également s'adresser directement à ces fournisseurs pour leur demander d'anonymiser leur version.

1.2 Protection des données – Questions d'ordre géneral

1.2.1 Code de conduite dans le domaine du pervasive computing

Durant le premier semestre 2006, nous avons participé à un échange de vues multidisciplinaire sur le thème du pervasive computing qui a réuni tant des experts en protection des données que des représentants d'associations de protection des consommateurs, d'universités, d'organisations ou de firmes privées. La collaboration de ces nombreuses personnes d'horizons différents a permis de définir des lignes générales pour l'utilisation des technologies du pervasive computing et des règles spécifiques dans trois secteurs d'applications possibles.

A l'initiative des organisations Stiftung Risiko-Dialog, Stiftung für Datenschutz und Informationssicherheit et ICT Switzerland, un dialogue multidisciplinaire dans le domaine du pervasive computing a eu lieu pendant le premier semestre 2006. Nous avons volontiers accepté l'invitation qui nous a été faite de participer à ces discussions, eu égard au potentiel d'atteinte à la vie privée inhérent à ces nouvelles technologies. L'objectif de ces échanges était notamment d'analyser les effets et les risques liés à ces applications et de définir des lignes générales dans ce domaine ainsi que des règles spécifiques pour certains secteurs particuliers tels que le domaine médical, le commerce de détail ou les transports.

Nous avons participé au groupe de travail traitant le secteur du commerce de détail. La principale application du pervasive computing dans ce domaine sera très probablement l'étiquetage de tous les produits avec des puces RFID. Une telle application permettra de localiser et d'identifier chaque produit de façon univoque sans qu'un contact visuel ne soit nécessaire. Ceci constituera notamment un nouvel instrument dans la lutte contre le vol. Les avantages pour les entreprises ne se limitent pas à cela: par exemple, l'inventaire du magasin s'en trouvera amélioré et simplifié. Il sera en outre facilement possible de tracer les déplacements des clients à l'intérieur du magasin, et donc d'optimiser la disposition des produits mis en vente.

Dans quelques pays, des entreprises ont déjà essayé d'introduire une telle application; les clients ayant vivement protesté contre ce qui était ressenti comme une atteinte excessive à la sphère privé, elles ont néanmoins été obligées de faire marche arrière.

Les discussions entre les différents partenaires ont permis de donner des orientations utiles, équilibrées et acceptables pour la mise en œuvre de telles applications.

Ce genre d'initiative est bienvenue et représente une bonne occasion pour chercher à réduire de façon proactive les problèmes potentiels d'atteinte à la sphère privée. Bien que les résultats de cet échange de vues soient encore trop vagues pour constituer un véritable code de conduite, la démarche est à notre avis un premier pas dans la bonne direction. Il est souhaitable que dans le futur les efforts soient poursuivis dans ce domaine.

1.2.2 L'engagement de drones de reconnaissance

Le Conseil fédéral a approuvé l'engagement de drones de reconnaissance et d'hélicoptères équipés de systèmes à infrarouges en faveur du Corps des gardes-frontière. Il convient néanmoins de créer maintenant la base légale pour l'engagement d'installations de surveillance de l'armée à des fins civiles.

Au cours de l'année précédente, nous avons déjà examiné la question de l'engagement de drones de reconnaissance. A la demande de l'administration des douanes, les drones de reconnaissance de l'armée devraient être mis en œuvre pour la reconnaissance aérienne dans les zones frontières au profit du Corps des gardes-frontière (cf. à ce sujet notre 13ème rapport d'activités 2005/2006, ch. 2.2.1). Nous estimons que ni la loi sur l'armée et l'administration militaire, ni la loi sur les douanes ne contiennent une base légale suffisante pour l'engagement de drones. Nous ne nous prononçons pas fondamentalement contre, mais nous avons demandé expressément que le Conseil fédéral d'une part autorise la surveillance et d'autre part qu'il fasse élaborer les bases légales suffisantes. Par contre, le Département fédéral des finances (DFF) a estimé que la loi sur les douanes constituait une base légale suffisante et s'est refusé à élaborer une proposition au Conseil fédéral en vue de la création d'une base légale.

Suite à cela, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a pris l'affaire en main et a préparé avec nous une proposition au Conseil fédéral. En juillet 2006, le Conseil fédéral a donné son accord à l'engagement de drones de reconnaissance et d'hélicoptères équipés de systèmes spéciaux à infrarouge (les Super Puma FLIR) pour surveiller les frontières nationales. Le système à infrarouges permet de déceler les sources de chaleur, donc de détecter et de poursuivre des personnes. Selon le Conseil fédéral, les deux systèmes de surveillance ne devraient être engagés que ponctuellement. Par ailleurs, selon cette décision du Conseil fédéral, il n'y aura pas d'enregistrements de données personnelles jusqu'à l'entrée en vigueur de la révision de la loi sur les douanes et de la révision de l'ordonnance

réglant la surveillance de la frontière verte au moyen d'appareils vidéo. Fort de cet appui du Conseil fédéral, le Corps des gardes-frontière et l'armée ont signé un contrat de prestations qui règle les processus, les responsabilités et les engagements.

Une motion sur le même sujet (05.3805) a été déposée, chargeant le Conseil fédéral de soumettre au Parlement une base légale au sens formel pour l'utilisation de drones par le Corps des gardes-frontière. Dans un co-rapport adressé au Conseil fédéral, nous avons souligné qu'il n'existait à ce jour aucune base légale pour l'engagement de drones. Dans sa prise de position de mai 2006, le Conseil fédéral a estimé que la nouvelle loi sur les douanes offrait une base légale formelle explicite pour l'engagement de moyens techniques de surveillance. Il a ajouté par ailleurs que, dans le cadre des dispositions d'exécution, il préciserait l'utilisation de ces moyens et s'assurerait que leur engagement respecte le principe de la proportionnalité.

Entre-temps, le Conseil fédéral semble avoir changé d'avis en ce sens qu'il s'est déclaré prêt à créer une base légale formelle pour l'engagement de moyens de surveillance à des fins civiles dans le cadre de la révision partielle de la législation militaire (plus précisément dans la future loi fédérale sur les systèmes militaires d'information) (voir ch. 1.2.3). La question de savoir quand, où et comment des installations de surveillance de l'armée pourront également être mises en œuvre à des fins civiles demeurera pour nous une préoccupation constante, à l'avenir aussi: en effet, le Conseil fédéral vient d'approuver l'engagement de drones de reconnaissance et d'hélicoptères Super Puma équipés de caméras à infrarouges (FLIR) dans le cadre de l'Euro 2008 (voir ch. 1.3.5).

1.2.3 Révision de la loi sur l'armée et l'administration militaire

Le Conseil fédéral a mis en consultation le projet de loi fédérale sur les systèmes militaires d'information. La plupart de nos Remarques ont été acceptées; de grandes divergences demeurent néanmoins en ce qui concerne les moyens de surveillance.

Au cours de l'année écoulée, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a poursuivi les travaux de révision de la loi sur l'armée et l'administration militaire, requis par le Conseil fédéral (cf. à ce sujet notre 13ème rapport d'activités 2005/2006; ch. 2.2.2). Le DDPS estime que cette révision doit aller de pair avec une adaptation des dispositions sur la protection des données figurant dans la loi sur l'armée. D'entente avec l'Office fédéral de la justice, nous avons défendu le point de vue selon lequel les différents systèmes d'information de l'armée et de l'administration militaire devraient être réunis dans une loi spécifique. Après s'être également rangé à cet avis, le DDPS a présenté un projet de loi fédérale sur les systèmes militaires d'information. Cette loi doit désormais constituer la base légale formelle des systèmes militaires d'information. Conformément à l'exigence de base légale suffisante posée par la loi sur la protection des données, cette nouvelle loi devra établir expressément pour chaque système d'information et dans les grandes lignes le but du traitement des données ainsi que son étendue. Elle devra aussi désigner les personnes participant au système d'information (personnes traitant les données, destinataires éventuels des données). Dans la mesure où des données sensibles ou des profils de la personnalité sont traités dans les systèmes d'information, les catégories de données traitées devront aussi être mentionnées dans la loi fédérale.

Au terme de longues discussions, nous avons trouvé un accord avec le DDPS sur la plupart des points et avons convenu de solutions conformes à la protection des données et acceptables pour les deux parties. Des divergences importantes subsistent néanmoins quant à l'utilisation des instruments de surveillance tels que les drones, les caméras thermiques et les détecteurs infrarouges. Nous nous sommes opposés à une disposition se contentant d'établir que «l'armée peut engager des appareils et des installations mobiles ou fixes, avec appui au sol ou appui aérien, avec ou sans pilote». Nous estimons que cela reviendrait à créer une clause générale pour toute forme de surveillance de l'État, quelle qu'elle soit, sans aucune restriction.

Dans un Etat de droit libéral démocratique, toute forme de surveillance étatique est une atteinte grave aux droits fondamentaux des citoyennes et citoyens. Les atteintes graves doivent être légitimées démocratiquement, donc prévues par une loi au sens formel. La loi fédérale doit spécifier le genre de surveillance et réglementer ses conditions-cadre. En d'autres termes, les appareils de surveillance utilisés doivent être nommément désignés et le genre et le but de la surveillance doivent figurer dans la loi fédérale. En outre, il faut établir tout aussi clairement quelles autorités sont habilitées à pratiquer cette surveillance et si elles peuvent également mener des actions de surveillance pour d'autres autorités ou même des particuliers. Ces exigences ne sont aucunement utopiques. Elles sont incontestées dans le domaine de la surveillance de la correspondance par poste et télécommunication par exemple: dans la loi fédérale du même nom (loi fédérale sur la surveillance de la correspondance par poste et télécommunication, LSCPT), le législateur a réglementé en détail l'admissibilité et les modalités de la surveillance. Nous demandons qu'il en soit de même pour les appareils de surveillance de l'armée.

Le DDPS a présenté le projet de loi fédérale sur les systèmes militaires d'information au Conseil fédéral. Celui-ci l'a soumis à un large débat dans le cadre d'une procédure de consultation. Nous pensons que la question de l'utilisation secrète ou notoire d'installations militaires d'information à des fins militaires ou civiles donnera lieu à de nombreuses discussions au plus tard lorsque la loi fédérale sur les systèmes militaires d'information sera soumise aux débats parlementaires.

1.2.4 Révision de l'ordonnance sur les douanes

Les données biométriques sont en principe des données sensibles. Une loi doit donc établir quelles données biométriques peuvent être traitées par une autorité et dans quel but. Dans le cadre de la révision de l'ordonnance sur les douanes, nous avons veillé à ce que les données biométriques – de même que les modalités de traitement – soient au moins détaillées dans les dispositions d'exécution.

Depuis quelques années, on assiste à une véritable expansion de l'utilisation des données biométriques. En effet, il s'agit là d'un domaine qui a subi une évolution imprévisible il y a peu de temps encore (par ex. l'intégration de données biométriques dans le passeport suisse, la banque de données sur les profils d'ADN). Dans le cadre de la consultation des offices relative à la loi fédérale sur les documents d'identité, nous avons déjà attiré l'attention sur cette évolution, qui n'est d'ailleurs pas terminée, et souligné le caractère extrêmement sensible des données biométriques. Pour cette raison, nous avons précisé que d'une manière générale, il faut qu'un texte légal formel, c'est-à-dire une loi fédérale, détermine les données biométriques pouvant être traitées par les autorités.

Dès lors, dans le cadre des travaux de révision de l'ordonnance sur les douanes, nous avons relevé que les caractéristiques biométriques retenues à l'art. 226 de cette ordonnance auraient dû, en fait, figurer dans la loi sur les douanes. Mais étant donné que la loi sur les douanes, récemment révisée, précise uniquement que le Conseil fédéral établit quelles données biométriques peuvent être relevées, nous avons demandé que l'ordonnance sur les douanes fixe et délimite avec précision les différentes données biométriques et les modalités de traitements autorisées (y compris une éventuelle transmission des données et la durée de leur conservation). Au terme de longues discussions, nous avons convenu avec l'administration des douanes des données biométriques pouvant être traitées en vue d'établir l'identité de personnes aux frontières. Il s'agit des empreintes digitales, des empreintes de la paume de la main, du profil d'ADN et des images faciales. Nous avons souligné qu'il était important à cet égard que soient mentionnées les lois fédérales qui règlent de façon détaillée le traitement des données biométriques. Nous nous sommes prononcés contre la collecte, à titre de réserve, d'images de l'iris par les autorités douanières. A notre connaissance, il n'existe aujourd'hui en Suisse aucune banque de données rassemblant des images de l'iris et ni l'Union européenne ni les Etats-Unis ne requièrent que cette caractéristique biométrique figure dans le passeport. Une collecte de ces données n'est donc pas opportune et serait contraire à la loi sur la protection des données.

Conformément à la loi sur les douanes, les entreprises de transport doivent permettre à l'administration des douanes de consulter tous les documents et relevés nécessaires au contrôle douanier. Cela permet aux autorités douanières de requérir des entreprises les listes de passagers et de marchandises. Nous sommes parvenus à imposer que ces listes ne soient pas conservées trois semaines, comme le souhaitait l'administration des douanes, mais seulement durant 72 heures.

1.2.5 La révision partielle de la loi sur les stupéfiants

Dans le cadre de la révision partielle actuellement en cours de la loi sur les stupéfiants, nous avons demandé que le traitement des données soit décrit avec plus de précision. Quant à la nouvelle compétence en matière d'annonce en cas de troubles liés à l'addiction, il convient de procéder à des améliorations législatives donnant plus de précisions sur le flux des données.

Après l'échec de la révision totale de la loi sur les stupéfiants en 2004, une initiative parlementaire veut mettre en œuvre les points qui étaient alors susceptibles de réunir une majorité. Le projet a notamment pour but de protéger la jeunesse, de renforcer les mesures de prévention et le rôle de la Confédération dans la coordination des efforts en matière de drogue.

Comme la loi sur la protection des données le requiert, le projet de révision contient une réglementation légale expresse du traitement des données personnelles. Toutefois, dans sa version première, le projet de loi était rédigé de manière si imprécise qu'il était difficile de déterminer dans quels cas il était possible de traiter des données personnelles dans le contexte des stupéfiants. Suite à ce constat, nous avons demandé au Conseil fédéral que le but du traitement des données, son étendue et les personnes y participant soient circonscrits avec davantage de précision. Il convient de retenir à titre complémentaire que la loi sur les stupéfiants ne prévoit ni d'accès en ligne (procédure d'appel), ni de communication régulière des données sous forme de listes.

Du point de vue de la protection des données, il convient en outre de souligner l'importance d'un nouvel instrument préventif de la politique nationale en matière de drogue, à savoir la compétence en matière d'annonce en cas de troubles liés à l'addiction: certains services et professionnels peuvent annoncer ces cas aux institutions de traitement ou aux services d'aide sociale. Mais il est regrettable que la loi ne dise pas dans quels cas on est en présence de troubles liés à l'addiction. Ce genre de système signifie obligatoirement que le traitement de données a lieu sur la base d'indices, notamment parce que le système d'annonce doit aussi être applica-

ble dès qu'apparaît le risque de troubles liés à l'addiction. En regard du principe de l'exactitude des données, il s'agit d'une démarche délicate, surtout parce que la supposition à la base du traitement des données est, en l'occurrence, très stigmatisante. Nous poursuivrons nos efforts pour que la marge d'appréciation quant à la décision de traiter des données soit réduite à un strict minimum par des mesures légales (au minimum au niveau de l'ordonnance).

1.2.6 Contrôles biométriques d'accès à des établissements de sport et de détente

L'examen des pratiques en matière de protection des données auprès des établissements de sports et de détente «KSS Sport- und Freizeitanlagen Schaffhausen» (ci-après KSS) a montré que l'utilisation des données biométriques pour contrôler l'accès aux établissements n'était pas entièrement conforme aux règles de la protection des données. Nous sommes donc intervenus pour que les données biométriques ne soient plus stockées de manière centralisée. En outre, une solution alternative doit être proposée aux clients qui ne souhaitent pas que leurs empreintes digitales soient relevées. Nous considérons que ces recommandations peuvent s'appliquer par analogie à d'autres établissements privés du même secteur qui utilisent des données biométriques pour leurs systèmes de contrôle d'accès.

KSS utilise depuis janvier 2005 un nouveau système afin de lutter contre l'utilisation frauduleuse des cartes d'abonnements nominatives, semestrielles ou annuelles, pour l'accès à la piscine et aux espaces de bien-être. En plus des données personnelles habituelles du client, les empreintes digitales de ce dernier de ce dernier sont relevées et enregistrées sous forme de gabarits biométriques (templates). Pour pénétrer dans l'établissement, le client doit insérer sa carte d'abonnement dans un lecteur asservissant le tourniquet d'entrée. Ensuite, l'abonné doit faire glisser son doigt sur un scanner intégré au lecteur de cartes, lequel se charge d'extraire un gabarit d'épreuve de l'empreinte digitale ainsi numérisée; celui-ci est comparé avec le gabarit de référence. Le tourniquet ne se libère qu'en cas de correspondance avérée (supérieure à un seuil minimal fixé) des deux gabarits biométriques considérés. Il était prévu que les gabarits soient enregistrés dans une base de données centralisée.

Eu égard à la relative sensibilité des données personnelles relevées pour contrôler l'accès à un établissement de sport et de détente, et étant donné les réactions négatives de certains clients refusant de fournir leurs données biométriques dans un tel contexte, nous avons effectué un contrôle. Dans le cadre de notre rapport final, nous avons notamment recommandé qu'une solution de rechange au même prix soit proposée aux abonnés s'opposant à ce que leurs données biométriques soient prélevées; pour les clients qui ne s'y opposeraient pas, nous avons recommandé que leurs données biométriques soient stockées sur une puce de la carte d'abonné plutôt que de façon centralisée. Nous avons également insisté sur la nécessité de fixer des délais d'effacement pour les données personnelles et les gabarits biométriques se rapportant à d'anciens clients. Nous avons également souligné l'importance de rendre anonymes les données transactionnelles («qui est entré quand») collectées par le système. Nous estimons que les données transactionnelles identifiables ne doivent pas être conservées dans le système central: pour accomplir les fonctions avancées du contrôle d'accès, la conservation des données identifiables est tout à fait suffisante sur la Smartcard de l'abonné; s'agissant des données transactionnelles collectées à des fins statistiques, leur centralisation doit avoir lieu sous une forme anonyme. KSS a accepté d'adapter son système à toutes nos recommandations dans un délai raisonnable et de suivre la plupart de nos propositions d'amélioration. Nous avons en outre demandé à KSS de nous informer lorsque toutes les mesures auront été réalisées, afin que nous puissions vérifier si elles correspondent bien aux recommandations formulées.

Le rapport intégral de ce contrôle (en allemand), ainsi qu'un résumé et un communiqué de presse ont été publiés sur notre site web. Une annexe a été ajoutée au rapport final; celle-ci rend compte des avis et des réponses de KSS au sujet du contrôle effectué ainsi que de notre appréciation finale.

1.2.7 Identification des personnes fréquentant les maisons de jeu

La Commission fédérale des maisons de jeu (CFMJ) nous a demandé si et dans quelle mesure une maison de jeu peut collecter, conserver et exploiter des informations se rapportant aux personnes fréquentant son établissement afin de détecter précocement les personnes susceptibles de devenir dépendantes du jeu. Nous avons estimé que la législation en vigueur ne permet pas un tel traitement de données. Une base légale est en principe souhaitable. Néanmoins les casinos pourraient invoquer un autre motif justificatif, tel qu'un intérêt privé ou public prépondérant. Dans tous les cas, un concept de protection des données doit être expressément prévu.

La Commission fédérale des maisons de jeu (CFMJ) s'est adressée à nous afin de nous demander si et dans quelle mesure un casino pouvait collecter, conserver et exploiter des informations se rapportant aux personnes fréquentant l'établissement afin de détecter précocement les personnes susceptibles de devenir dépendantes du jeu. Il s'agissait en particulier d'examiner si les informations recueillies à d'autres fins (marketing, lutte contre le blanchiment d'argent) pourraient également être utilisées dans le cadre de la mise en œuvre du concept social.

La collecte, la conservation, l'exploitation d'informations se rapportant aux personnes fréquentant un casino constituent un traitement de données personnelles au sens de la Loi fédérale sur la protection des données (LPD). En tant que personnes privées, les casinos doivent pouvoir se fonder sur l'un des motifs justificatifs de l'art. 13 LPD, à savoir le consentement de la personne concernée, un intérêt privé ou public prépondérant ou une base légale. De son côté, pour pouvoir imposer un tel traitement de données aux casinos, la CFMJ doit – en tant qu'organe fédéral – nécessairement disposer d'une base légale (art. 17 LPD).

Nous avons donc commencé par examiner si en l'occurrence, la législation en vigueur prévoit un tel traitement de données. Nous avons constaté que la loi fédérale sur les maisons de jeu (LMJ) oblige les casinos à mettre en oeuvre un programme de mesures sociales; l'ordonnance d'exécution de cette loi précise que les casinos doivent prendre des mesures en fonction de critères d'observation préalablement définis. Nous avons cependant estimé que les traitements de données mis en œuvre par les casinos pour prévenir les conséquences dommageables du jeu sur le plan social doivent être expressément prévus dans une base légale formelle. Les informations collectées ayant trait à la santé, elles constituent des données sensibles au sens de la LPD.

Les casinos disposent d'informations qui sont collectées en application de la Loi fédérale sur le blanchiment d'argent (LBA). Les casinos, respectivement la CFMJ, ne peuvent cependant se fonder sur ces bases légales pour utiliser les données personnelles dans le cadre de l'application du concept social, à d'autres fins que la lutte contre le blanchiment d'argent. Les casinos ont également la possibilité d'enregistrer les données de leurs clients à des fins de marketing, pour autant que ceux-ci y consentent. En vertu du principe de finalité, les données collectées ne peuvent cependant être utilisées qu'à des fins de marketing et seulement si la personne concernée a donné son consentement libre et éclairé. En conclusion, la CFMJ et les casinos ne disposent pas de base légale suffisamment précise pour justifier d'autres traitements de données que ceux expressément mentionnés dans la législation spéciale.

Cependant, les casinos pourraient en tant qu'entités privées se fonder sur un autre motif justificatif, à savoir le consentement de la personne concernée ou un intérêt privé ou public prépondérant et utiliser les données à disposition dans le contexte du concept social. Un tel traitement de données doit cependant respecter les principes généraux de la protection des données, en particulier les principes de finalité, de proportionnalité et de transparence.

En tout état de cause, nous avons estimé qu'une nouvelle base légale serait souhaitable pour pouvoir utiliser les instruments existants à des fins de détection précoce de personnes dépendantes du jeu. Le caractère sensible des données traitées dans le cadre du concept social et l'intérêt public poursuivi sont autant de raisons pour une base légale claire. En outre, la détermination d'un cadre juridique permettrait de garantir que tous les casinos mettent en oeuvre le concept social avec la même efficacité.

Nous avons finalement relevé que les casinos doivent dans tous les cas prévoir un concept pour les traitements de données effectués au sein de leurs établissements. Ils doivent en particulier déterminer les données collectées, leur finalité ainsi que leur durée de conservation; de même, l'accès éventuel des autorités ou de tiers doit être réglementé et une information des personnes concernées s'impose, conformément au principe de transparence.

1.2.8 Systèmes d'accès électronique dans les domaines skiables et protection des données

Des systèmes de plus en plus sophistiqués contrôlent l'accès aux domaines skiables et soulèvent des problèmes de protection des données. Lors de l'achat d'un abonnement, le skieur doit remettre ses coordonnées et une photographie. La collecte et l'utilisation de ces données personnelles doivent respecter la législation sur la protection des données. Les exploitants d'installations de sports d'hiver ne peuvent se prévaloir d'un intérêt privé prépondérant pour afficher publiquement les données personnelles des titulaires d'abonnement. D'autres moyens plus respectueux de la sphère privée permettent de vérifier la validité des abonnements et d'éviter les abus.

Lors de l'achat d'un abonnement, le skieur doit fournir une photographie ainsi que des informations sur sa personne. La collecte et l'utilisation de ces données personnelles constituent un traitement de données au sens de la loi sur la protection des données (LPD), dont les dispositions sont applicables. Les exploitants d'installations de sports d'hiver recourent de plus en plus à des systèmes électroniques de contrôle d'accès. Dans certaines stations, la photo du détenteur de l'abonnement apparaît alors sur un écran lorsque l'usager franchit le portillon. Un tel système vise d'une part à contrôler si le détenteur et le porteur de l'abonnement sont bien une seule et même personne, d'autre part à vérifier la validité de l'abonnement. Généralement, le contrôle est effectué par le personnel de la station, mais dans certains domaines skiables, l'écran est également visible pour les tiers qui se trouvent à proximité du point de contrôle. Les données personnelles du titulaire de l'abonnement apparaissent alors à l'écran et y restent visibles jusqu'au passage du client suivant, ce qui peut durer plusieurs minutes. Un certain nombre de personnes se sont adressées à nous pour se plaindre de l'affichage public de leurs données personnelles. Nous avons examiné si ce procédé était conforme à la LPD.

Toute personne a droit au respect de sa sphère privée et a en particulier le droit de préserver son identité à l'égard des tiers, y compris dans le cadre de ses loisirs. De son côté, un particulier effectuant un traitement de données personnelles peut se prévaloir d'un motif justificatif: ce peut être une loi, un intérêt privé ou public prépondérant, ou encore le consentement des personnes concernées. Même s'il existe un motif justificatif, les principes généraux de la protection des données s'appliquent.

L'exploitant d'une station de sports d'hiver dispose-t-il d'un motif justificatif lui permettant d'afficher à l'écran les données des titulaires d'un abonnement de ski de façon également visible pour des tiers? Aucune loi n'existe dans ce domaine et aucun intérêt public ne peut être invoqué. Ne restent dès lors, à titre de motifs justificatifs, qu'un intérêt privé prépondérant ou le consentement des personnes concernées.

L'exploitant d'une station de sports d'hiver a bien un intérêt légitime à vérifier la validité des abonnements et à contrôler que des tiers n'utilisent pas abusivement des abonnements non transmissibles. A cette fin, il a le droit d'installer des systèmes électroniques de contrôle d'accès. Ce faisant, il doit également respecter les principes généraux de la protection des données, en particulier les principes de finalité, de proportionnalité et de transparence. En l'occurrence, nous estimons qu'il est douteux qu'un affichage public permette de vérifier la validité des abonnements. Il ne revient pas aux autres clients de contrôler, en lieu et place du personnel, qu'aucun abus n'est commis. Il semble plutôt que le recours à de tels systèmes ait pour objectif de dissuader d'éventuels resquilleurs; or, en cas d'abus, ce ne sont pas les données personnelles du skieur qui s'affichent, mais celles du titulaire de l'abonnement qui n'a pas forcément connaissance de l'abus et est ainsi injustement stigmatisé.

De plus, conformément au principe de la proportionnalité, il convient autant que possible d'appliquer la mesure qui préservera le plus la sphère privée. L'affichage public de données personnelles représente une intrusion non négligeable dans la sphère privée des personnes concernées. Dans le cas présent, une telle mesure ne respecte pas le principe de la proportionnalité, car il existe d'autres moyens de contrôle à la fois efficaces et conformes aux impératifs de la protection des données, par exemple les contrôles systématiques ou ponctuels effectués par des employés; seul le personnel doit avoir accès aux écrans.

Compte tenu de ces considérations, les exploitants d'installations de sports d'hiver ne peuvent pas invoquer un intérêt privé prépondérant à l'affichage public de données personnelles. Le seul motif justificatif restant serait le consentement des personnes concernées. Un tel consentement doit être donné librement et en connaissance de cause: le client doit pouvoir s'opposer au traitement de ses propres données sans qu'il en résulte pour lui un désavantage quelconque. L'affichage public des données personnelles devrait alors être facultative, ce qui serait techniquement possible mais contrarierait les intentions de contrôle de l'exploitant.

Nous sommes arrivés à la conclusion que l'affichage public de la photographie et de l'identité des usagers d'installations de sports d'hiver à des fins de contrôle n'est pas conforme à la législation sur la protection des données. La communication de données personnelles à des tiers n'est en effet pas nécessaire et contraire au principe de proportionnalité. D'autres moyens plus respectueux de la sphère privée permettent de vérifier la validité des abonnements et d'éviter les abus, par exemple les contrôles systématiques ou sporadiques tels que les connaissent les transports en commun. Nous avons rendu les personnes concernées attentives à leur droit de déposer plainte en vertu de l'art. 15 LPD.

1.2.9 Contrôle du règlement de traitement pour le système d'information PLASTA

Lors des contrôles de règlements de traitement que nous effectuons, nous constatons très souvent des lacunes au niveau de l'application des mesures organisationnelles et techniques. Ces lacunes concernent principalement le cryptage et la journalisation, mais également les procédures de contrôle et la documentation des processus (déroulements). Les exigences concernant le contenu d'un règlement de traitement sont accessibles sur notre site web.

Le système d'information PLASTA du Secrétariat d'État à l'économie (SECO) est utilisé pour le placement et pour les statistiques du marché du travail. L'exploitation d'un tel système requiert l'élaboration d'un règlement de traitement. Ce règlement a été élaboré par le SECO conformément aux exigences que nous avons publiées sur notre site web (cf. www.edoeb.admin.ch, Documentation – Protection des données – Brochures – Mesures techniques et organisationnelles).

Nous avons contrôlé ce règlement et constaté que certains points étaient susceptibles d'être améliorés.

La description des interfaces qui représente entre autres le flux des informations entre le système PLASTA (SECO) et les unités d'organisation utilisant le système ne décrit pas partout les champs de données mentionnés ci-dessous: DE (d'où proviennent les données?, par ex. PLASTA/SECO); A (à qui les données sont-elles transmises, par ex. aux centres de placement régionaux); BUT (dans quel but les données sont-elles communiquées?); TYPE DONNÉES (quelles données [ou types de données] sont communiqués?); PÉRIODICITÉ (à quelle fréquence les données sont-elles communiquées?); INITIATEUR (qui entame la communication des données?); MEDIA (par quel moyen de communication ou support les données sont-elles communiquées?).

En outre, la liste des documents système et de projet qui ont été élaborés n'est qu'approximative. Une énumération exhaustive des documents qui ont été élaborés pour la planification et la réalisation du système ainsi que pour l'exploitation manque. Une telle liste contribuerait pourtant à assurer une certaine transparence et traçabilité.

Les processus et les groupes de processus sont mentionnés dans le règlement, mais pour des informations plus détaillées, ce dernier renvoie à l'intranet. Nous avons cependant constaté que certaines données, notamment les schémas de processus, n'y sont pas accessibles et que certaines descriptions de processus, par ex. les processus de contrôle, manquent (la protection des données fait une distinction entre les processus traditionnels nécessaires à l'accomplissement des tâches, les processus de contrôle et les processus utilisés pour faire valoir le droit d'accès).

Au niveau des procédures de contrôle, il est nécessaire de préciser quels contrôles ont déjà été effectués dans la phase de planification et de réalisation et lesquels sont encore prévus pour la phase d'exploitation. Ensuite, dans la phase d'exploitation, on devra indiquer quels contrôles ont été effectués. Les procédures de contrôle comprennent entre autres des dépouillements de fichiers journaux. Il y a lieu de documenter qui dépouille quels fichiers journaux et quand.

Nous avons soumis nos recommandations au SECO et l'avons prié en même temps de mettre à jour le règlement et de nous faire parvenir un exemplaire de la version révisée.

Sur la base des expériences faites à ce jour, nous procéderons dorénavant plus souvent à des contrôles de règlements de traitement.

1.3 Justice/Police/Sécurité

1.3.1 La lutte contre le hooliganisme

Depuis quelque temps, des actes de violence lors de manifestations sportives peuvent également être observés en Suisse. Pour combattre ce problème, la Confédération a entamé en 2002 des travaux de législation. Les dispositions qui en résultent sont contenues dans la loi fédérale sur les mesures visant au maintien de la sûreté intérieure (LMSI) et dans l'ordonnance qui s'y rapporte (OMSI) et sont entrées en vigueur le 1er janvier 2007.

Les nouvelles dispositions dans le domaine de la lutte contre le hooliganisme prévoient d'une part la création d'une banque de données dans laquelle sont enregistrées des informations concernant des personnes qui ont «affiché un comportement violent» lors de manifestations sportives (art. 24a al.1 LMSI). D'autre part, ces dispositions prévoient diverses mesures telles que l'interdiction de périmètre, l'interdiction de se rendre dans un pays donné, l'obligation de se présenter à la police et la garde à vue. Du point de vue de la protection des données, nous devons relever deux points délicats:

Le premier concerne certaines incertitudes concernant les conditions devant être remplies pour qu'une personne puisse être enregistrée dans cette banque de données. A première vue, le texte de la loi LMSI semble être bien clair; malheureusement, cette clarté disparaît dès qu'on lit les articles 21a et 21b de l'ordonnance. L'article 21a énumère un nombre d'infractions qui sont considérées comme «comportement violent». Cette liste ne contribue pas à la clarté puisque avec le mot «notamment» dans le texte de loi, elle ne doit pas être considérée comme exhaustive. L'article 21b de l'ordonnance contribue encore à ce flou en stipulant qu'une interdiction de stade prononcée par une fédération ou association sportive est considérée comme preuve d'un comportement violent (art. 21b, al. 1, lit. c). Cette disposition peut s'avérer très problématique, étant donné que de telles interdictions de stade peuvent être prononcées de manière absolument arbitraire et qu'il n'existe aucun moyen de recours.

Le deuxième point qui pose problème dans le contexte de la protection des données est le manque de clarté des dispositions qui régissent la communication des données à des personnes privées (par ex. aux exploitants de stades sportifs) ainsi que les traitements de données effectués par ces derniers. Le seul fait déjà que des données issues d'une banque de données étatique soient communiquées de manière régulière et en grand nombre à des personnes privées n'est pas sans poser problème. C'est

la raison pour laquelle le législateur a prévu que le Conseil fédéral fixerait les modalités du «traitement des données par les destinataires et par des tiers» (art. 24a al. 8 LMSI). L'ordonnance ne remplit cependant aucunement ce mandat légal. Elle déplace même le problème à un niveau normatif inférieur. L'article 21k de l'ordonnance stipule en effet que le Service d'analyse et de prévention (SAP) règle dans un règlement de traitement «l'utilisation et le traitement des données par les organisateurs de manifestations sportives». Malheureusement, le règlement de traitement ne contient pas non plus les règles nécessaires. Son article 27 al. 3 stipule que «conjointement avec les organisateurs sportifs, le SAP établit des directives relatives aux conditions liées à la transmission des données par les organisateurs sportifs ». Cette disposition est à critiquer car elle poursuit la cascade des délégations sans contribuer à la clarté. Au contraire, elle crée encore plus d'incertitude puisqu'elle mentionne une «transmission des données par les organisateurs sportifs». Nous ne sommes à ce jour pas en mesure de prévoir comment et quand ces questions ouvertes trouveront réponse.

1.3.2 Projet pilote d'index national de police

La mise en place d'un projet pilote d'index national de police n'a été possible qu'avec l'entrée en vigueur anticipée de l'article 17a de la loi sur la protection des données. Nous avons émis un avis favorable pour le cas d'espèce et avons annoncé que nous effectuerons des visions locales auprès des différents utilisateurs afin de vérifier si les conditions fixées pour cet essai pilote sont respectées.

L'Office fédéral de la police (fedpol) nous a consultés en été 2006 sur la mise en place d'un projet pilote d'index national de police. Les bases légales invoquées n'étant pas adéquates et le nouvel article 17a de la loi fédérale sur la protection des données (LPD) relatif aux projets pilotes n'étant pas encore en vigueur, nous avons indiqué à fedpol qu'un tel projet pilote ne pouvait pas être entrepris. Fedpol a alors proposé une entrée en vigueur anticipée du nouvel article 17a LPD. La proposition contenait également un avis de l'Office fédéral de la justice selon lequel une seule disposition pouvait tout à fait entrer en vigueur avant l'ensemble des normes révisées d'une loi. L'ordonnance sur l'exploitation pilote de l'index national de police et l'ordonnance sur la mise en vigueur anticipée de l'article 17a LPD sont en vigueur depuis le 15 décembre 2006. Nous avons émis un avis favorable après avoir constaté, sur la base des informations fournies par fedpol, que les conditions fixées par cette nouvelle disposition pour la mise en place du projet pilote étaient remplies; nous avons rappelé à l'office qu'il devra transmettre un rapport d'évaluation au Conseil fédéral au plus tard deux ans après la mise en œuvre de la phase d'essai. Nous avons souligné que le projet pilote d'index national de police est un cas particulier en raison de l'entrée en vigueur anticipée de l'art. 17a LPD. Nous avons également indiqué que des normes d'application concernant l'art. 17a LPD devront être élaborées dans le cadre de la révision de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Nous avons précisé que notre avis concernant le projet pilote d'index national de police avait un caractère exceptionnel et qu'il ne pourrait servir de précédent. A l'avenir, certains points pourraient être évalués de manière différente, par exemple la liste des participants au projet pilote ou les données utilisées dans le cadre du projet pilote. Finalement, nous avons annoncé à fedpol que nous effectuerons des visions locales auprès d'un utilisateur interne de l'office, d'un utilisateur du Corps des gardes-frontière et, avec la collaboration de l'autorité cantonale de protection des données, auprès d'un utilisateur cantonal.

1.3.3 Le droit d'accès indirect

Dans une décision du 31 août 2006, la Commission fédérale de la protection des données et de la transparence (CFPDT) a retenu que le «droit d'accès indirect» ne satisfaisait pas aux exigences de la Convention européenne des droits de l'homme (CEDH). C'est notamment dans les cas dans lesquels une mise en danger de l'ordre constitutionnel libéral et démocratique de la Suisse ou de l'existence, de l'indépendance et de la sûreté de la Confédération et des cantons peut être exclue qu'il est absolument indispensable que les personnes concernées soient informées du traitement qui est effectué avec leurs données. Sur la base de cette décision, nous avons adapté notre pratique.

En rapport avec le «droit d'accès indirect», la Commission fédérale de la protection des données (appelée nouvellement «Commission fédérale de la protection des données et de la transparence»; CFPDT) a rendu un nouveau jugement. Nous tenons tout d'abord à préciser qu'il ne s'agit pas en l'occurrence d'un véritable droit d'accès indirect puisque la personne concernée qui a déposé une demande de renseignement reçoit en principe de notre part une réponse au libellé toujours identique qui ne lui permet pas de savoir si elle est enregistrée ou non (cf. notre 7ème rapport d'activités 1999/2000, ch. I. 1.2). La décision de la CFPDT concerne cependant l'application de la règle d'exception prévue à l'article 18 al. 3 de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). En vertu de cet article, nous pouvons déroger à la réponse stéréotype prévue par la loi et, à titre exceptionnel, fournir à la personne requérante des renseignements de manière appropriée, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen d'empêcher que ces personnes soient lésées gravement et de manière irréparable.

Dans ses considérants, la CFPDT a tout d'abord retenu que l'article 18 LMSI ne prévoyait en principe aucun droit de la personne concernée d'être renseignée, mais seulement un contrôle administratif particulier et indépendant, effectué en première instance par le PFPDT et en deuxième instance par la CFPDT. Ce n'est qu'à titre exceptionnel qu'une information selon l'article 18 al. 3 LMSI peut être envisagée. De plus, les personnes enregistrées devraient être informées après coup sur le traitement des données, ceci conformément à l'article 18 al. 6 LMSI et seulement «pour autant que cela n'entraîne pas un volume de travail excessif». La CFPDT a ensuite critiqué que les accusés de réception que nous envoyons automatiquement aux personnes con-

cernées après avoir reçu leur demande de renseignement indirecte ne mentionnent pas de manière explicite qu'une information adéquate peut être fournie en cas de dommage grave et irréparable. Ceci impliquerait que la majorité des personnes qui déposent une demande n'ont aucune chance d'être renseignées à titre exceptionnel en vertu de l'article 18 al. 3 LMSI.

La CFPDT a ensuite examiné la disposition de l'article 18 al. 3 LMSI également sous l'angle du droit constitutionnel et du droit public international en se référant à des décisions du Tribunal fédéral et de la Cour européenne des droits de l'homme. D'après la CFPDT, il résulte de ces jugements qu'un seul soupçon ou un faux renseignement donné par un agent de police représentent un grave préjudice, qui ne ferait qu'être renforcé par la communication standard prévue par l'article 18 LMSI. Selon la CFPDT, c'est notamment dans les cas dans lesquels une mise en danger de l'ordre constitutionnel libéral et démocratique de la Suisse ou de l'existence, de l'indépendance et de la sûreté de la Confédération et des cantons peut être exclue qu'il est indispensable que les personnes concernées soient informées d'un traitement de données. La CFPDT a donc conclu que les articles 18 al. 1 et 2 LMSI ne répondaient pas aux exigences de la Convention européenne des droits de l'homme (CEDH).

La CFPDT relève également que la règle pour les cas exceptionnels prévue à l'art. 18 al. 3 LMSI est si irrationnelle et inadéquate pour l'objectif visé qu'elle ne permet manifestement pas au PFPDT d'appliquer une pratique raisonnable qui prenne en compte aussi bien la protection des droits fondamentaux que les objectifs de l'art. 1 LMSI. Elle retient en outre que le fait d'exclure pratiquement la possibilité d'être renseigné n'est pas compatible avec la protection des droits fondamentaux telle qu'elle est prévue dans la CEDH et la Constitution fédérale.

Se fondant sur ces considérants, la CFPDT nous a recommandé dans de tels cas d'informer la personne requérante selon l'art. 18 al. 3 LMSI du fait qu'elle n'était pas enregistrée. Elle nous a également recommandé de modifier les modalités d'information des personnes déposant une demande de renseignement concernant les traitements des données de police effectués par la Confédération, de manière à ce que nous soyons en mesure de fournir des renseignements, conformément à sa décision. Parallèlement, la CFPDT a recommandé à l'Office fédéral de la police d'engager, dans le cadre de l'actuelle révision de la LMSI, une modification du droit d'être renseigné pour que celui-ci devienne conforme à la CEDH.

Nous avons donc modifié en conséquence nos accusés de réception pour les demandes de renseignement indirectes. Nous rendons ainsi la personne requérante attentive au fait que la réponse stéréotypée est prévue par la loi et qu'elle ne lui permet pas de savoir si elle est enregistrée dans le système d'information ou non. En même temps, nous attirons explicitement l'attention de la personne concernée sur la règle prévue à l'art. 18 al. 3 LMSI pour les cas exceptionnels et sur le fait qu'elle peut faire valoir dans les 30 jours qu'elle subirait un dommage irréparable au cas où elle ne recevrait pas d'information appropriée. Finalement, nous avons tenu compte des considérants de la CFPDT relatives à l'art. 18 al. 3 LMSI pour notre pratique et examinerons dorénavant de cas en cas si les conditions stipulées dans cette disposition sont remplies ou non.

1.3.4 Augmentation de la durée de conservation des données de communication

Dans le cadre d'un rapport du Conseil fédéral donnant suite à un postulat intitulé «lutter plus efficacement contre le terrorisme et le crime organisé», nous avons été invités à prendre position notamment sur la question de l'augmentation de la durée de conservation des données de communication de six à douze mois. Nous estimons qu'une telle mesure est disproportionnée.

La Commission de la politique de sécurité des Etats a demandé au Conseil fédéral d'examiner les modifications à apporter à la législation afin de lutter plus efficacement contre le terrorisme et le crime organisé. La commission estimait notamment que le délai de six mois s'appliquant à la conservation des données en vue d'un contrôle rétroactif des communications était trop court. Dans le cadre de son rapport en réponse à ce postulat, le Conseil fédéral a proposé de prolonger le délai de six à douze mois à l'occasion d'une adaptation ultérieure de la législation (Loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT)). Nous avons été invités à prendre position sur les conclusions de ce rapport.

La conservation systématique et obligatoire des données constitue une restriction importante de la protection de la sphère privée et doit être pleinement justifiée. Nous estimons que le délai actuel de six mois est largement suffisant et sommes par conséquent qu'une prolongation de ce délai serait disproportionnée. Dans les cas d'entraide judiciaire internationale notamment, il serait envisageable de demander à l'organe compétent le blocage des données, dès réception de la requête, afin de préserver l'intégralité du délai.

En outre, nous nous sommes également référés à l'avis du Groupe de travail «Article 29» du 21 octobre 2005 sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données.

(http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_fr.pdf)

Nous avons souligné que si la durée de conservation des données devait être malgré tout étendue à douze mois, il conviendrait au moins de limiter l'application de cette mesure dans le temps et de procéder à une évaluation de l'efficacité de la mesure envisagée après une période déterminée.

1.3.5 Les activités du PFPDT en rapport avec l'Euro 08

Dans le cadre des préparatifs pour l'Euro 08, on nous a prié à diverses reprises de prendre position. Les thèmes soulevés ont été d'une part la décision du Conseil fédéral relative au service d'appui de l'armée, d'autre part l'accréditation et le marketing sauvage.

En été 2006, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) nous a demandé de prendre position sur le projet de décision du Conseil fédéral relatif au service d'appui de l'armée. Dans notre prise de position, nous avons relevé que les indications concernant la protection de l'espace aérien étaient fortement imprécises et qu'une réglementation plus détaillée était de rigueur si le service d'appui prévoyait d'engager des drones. Etant donné que l'objectif de l'engagement de drones et d'hélicoptères équipés de systèmes de reconnaissance aérienne à infrarouges est uniquement de coordonner l'engagement des forces de sécurité ou éventuellement des équipes de secours, il n'est pas nécessaire d'enregistrer les images ou même de les transmettre à autrui. C'est pourquoi la décision du Conseil fédéral interdit l'enregistrement des informations, ce qui est conforme au principe de la proportionnalité (cf. ch. 1.2.2).

En été 2006 également, nous avons présenté au Secrétariat d'Etat à l'économie (SECO) nos remarques concernant la révision de la loi fédérale contre la concurrence déloyale (LCD), qui était alors en cours. Il s'agissait de nouvelles dispositions devant être élaborées pour lutter contre ce qu'on appelle le «marketing sauvage» ou «marketing parasitaire». L'aspect qui importait pour la protection des données dans ce projet – qui a entre-temps été enterré – était le fait que les flux de données qui auraient été introduits en vertu de cette loi n'avaient absolument pas été définis. L'objectif était plutôt d'autoriser - au moyen de formulations très générales - la communication des données par les divers organes devant appliquer la loi, sans pour autant donner de précisions sur les flux de données. Le tout était formulé dans un article qui aurait dû être publié sous le titre «entraide administrative en Suisse». Ces dispositions auraient cependant été en nette contradiction avec la nature de l'entraide administrative car celle-ci a été instituée pour régler l'ensemble des flux de données nécessaires à l'application et non pas seulement des cas isolés.

En automne 2006, suite à une demande de l'Office fédéral de la police (fedpol), nous nous sommes prononcés sur les contrôles de sécurité effectués dans le cadre de la procédure d'accréditation pour l'Euro 08. La question soulevée était la participation de l'Etat à cette procédure de l'UEFA qui prévoyait que les autorités fédérales interrogent certaines banques de données gouvernementales pour émettre ensuite une

recommandation à l'UEFA pour les personnes concernées. Il était prévu d'interroger les banques de données suivantes: le système de traitement de données relatives à la protection de l'Etat (ISIS), le système d'information prévu pour la lutte contre le hooliganisme HOOGAN, le casier judiciaire informatisé VOSTRA, le système de recherches informatisées de police RIPOL, le système d'information Schengen ainsi que le système d'information central sur la migration SYMIC. Quant au nombre de personnes concernées par une procédure d'accréditation, on l'estimait à 25'000. Il s'agissait en premier lieu de collaborateurs de l'UEFA et du comité d'organisation de l'Euro 08, d'invités de l'UEFA, de membres des équipes et leurs accompagnants, ainsi que de journalistes et de personnel de sécurité et de service.

L'examen devait porter sur la question de savoir si les activités gouvernementales, à savoir les interrogations des banques de données et l'émission de recommandations à l'UEFA, trouvaient un fondement suffisant dans le consentement de la personne concernée.

Nous avons tout d'abord déclaré que le consentement pouvait être considéré comme problématique dans le contexte donné. Ceci premièrement parce qu'un consentement doit être donné de plein gré, deuxièmement en connaissant les conséquences qui peuvent en résulter. Or, le fait que ces personnes soient employées permet de douter que leur consentement soit toujours de plein gré. Il ne faut pas oublier non plus que ces personnes courent en plus le risque de se faire licencier par leur employeur au cas où la recommandation serait négative. Compte tenu de ces considérations ainsi que du nombre considérable de personnes concernées, nous avons conclu, en accord avec l'Office fédéral de la justice, que le consentement des personnes concernées n'était pas suffisant pour permettre la participation étatique à la procédure d'accréditation et donc qu'une base légale particulière était nécessaire. Celle-ci doit revêtir la forme d'une loi puisque l'interrogation des systèmes d'information mentionnés constitue un traitement de données personnelles sensibles. Une telle base légale permettant de communiquer des données à des personnes privées n'existe cependant que pour le système d'information HOOGAN.

A part ces prises de position, nos travaux dans le cadre de l'EURO 08 nous ont également menés à poursuivre nos contacts avec les divers organes et personnes impliqués dans l'organisation de cette manifestation afin de discuter les traitements de données prévus. Citons notamment l'UEFA, l'Office fédéral du sport (OFSPO) ainsi que fedpol.

1.3.6 Modification des ordonnances pour l'échange de données avec Europol

Dans le cadre de la consultation des offices, nous avons pris position sur l'entrée en vigueur de l'art. 351novies du Code pénal et sur la modification des ordonnances concernant l'échange de données avec Europol. Nous avons estimé qu'une simple modification des ordonnances n'était pas suffisante.

Dans le cadre de la consultation des offices, nous avons eu l'occasion de prendre position sur le projet de modification de diverses ordonnances devant être adaptées afin de permettre l'échange de données avec l'office européen de la police (prévu par l'Accord Europol). Nous avons rappelé que la base légale formelle sur laquelle se fondent toutes les banques de données concernées était trop générale (cf. notre 12ème rapport d'activités, ch. 3.1.2). Selon la LPD, le traitement de données sensibles et des profils de personnalité nécessite en effet une base légale formelle, qui doit préciser au moins la finalité du traitement et son importance. Nous avons relevé qu'une simple modification des ordonnances relatives aux banques de données concernées n'est pas suffisante. Cette remarque n'a pas été prise en compte mais a été mentionnée comme divergence dans la requête au Conseil fédéral. La plupart de nos autres remarques ont cependant été prises en compte.

1.3.7 Projet de loi sur les systèmes d'information de police

Le projet de loi sur les systèmes d'information met sous un même toit les bases légales régissant des fichiers de police existants comme RIPOL, IPAS et JANUS. Il ne crée qu'un seul nouveau système de traitement de données: l'index national de police, qui est un répertoire des bases de données existantes. Si, dans l'ensemble, nos remarques ont été prises en compte, nous regrettons le maintien du système dit du «droit d'accès indirect». Ce dernier ne permet pas à la personne qui en fait la demande de savoir si des données la concernant sont contenues dans les fichiers de l'Office fédéral de la police soumis à une telle procédure et, cas échéant, d'y avoir accès.

Dès 2003 nous avons été consultés à plusieurs reprises dans le cadre de l'élaboration du projet de loi sur les systèmes d'information de police et nous avons pu faire part de nos remarques et propositions. Ce projet améliore la transparence dans le domaine complexe des systèmes d'information de police de la Confédération, systèmes auxquels les cantons ont de plus en plus accès. La transparence est aussi un élément

essentiel du respect au droit à la protection des données. A l'exception de l'index national de police, qui est un répertoire des bases données existantes, le projet ne crée pas de nouveaux systèmes de traitement des données (cf. aussi à ce sujet ch. 1.3.2). Il permet de mettre sous un même toit les bases juridiques régissant les fichiers existants, en particulier RIPOL, IPAS et JANUS. Si, dans l'ensemble, nos remarques ont été prises en compte, nous avons fermement contesté le maintien du système dit du «droit d'accès indirect». Ce système est actuellement prévu dans la loi sur les offices centraux de police criminelle de la Confédération (LOC) et dans la loi instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Il ne permet pas à la personne qui en fait la demande de savoir si des données la concernant sont contenues dans les fichiers de l'Office fédéral de la police soumis à une telle procédure et, cas échéant, d'y avoir accès. Le système dit «du droit d'accès indirect» lui donne uniquement la faculté de nous demander de vérifier si des données la concernant sont traitées conformément au droit par la l'Office fédéral de la police dans les systèmes d'information ISIS, JANUS et GEWA. Nous communiquons au requérant une réponse, au libellé toujours identique, selon laquelle aucune donnée le concernant n'a été traitée illégalement, ou que nous avons adressé au responsable du traitement la recommandation de remédier à une erreur commise dans le traitement des données. Le requérant ne sait jamais, sauf rares exceptions, s'il est enregistré dans les systèmes en question et cas échéant, quelles données le concernant sont traitées. Les droits de la personne concernée sont ainsi mis entre parenthèses et dans ces conditions on ne saurait parler de «droit d'accès indirect». Il s'agit uniquement d'un droit de demander à une autorité de contrôle de vérifier la licéité du traitement. Ce système est insatisfaisant du point de vue de la protection des données. D'une part, nos vérifications n'ont qu'une portée limitée et l'information des personnes concernées est quasi inexistante. D'autre part, la pratique actuelle 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 (à ce sujet, voir également ch. 1.3.3.). Outre cette divergence majeure, nous avons critiqué le fait qu'une information ultérieure des personnes concernées n'est prévue que lorsque les données ont été recueillies directement (et à leur insu) par la police judiciaire fédérale (cf. également ch. 1.3.8). Nous avons également 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.

1.3.8 Contrôles dans le domaine de l'information ultérieure des personnes concernées

En rapport avec la procédure d'information ultérieure des personnes concernées, le DFJP a décidé que l'article 14 al. 1 LOC n'était applicable que dans les cas où l'Office fédéral de la police recueillait lui-même des données à l'insu des personnes concernées.

En rapport avec la procédure d'information ultérieure des personnes concernées dans le domaine policier et nos recommandations à ce sujet, nous avons porté l'affaire devant le Département fédéral de justice et police (DFJP) pour prise de décision (cf. notre 13ème rapport d'activités 2005/2006, ch. 3.1.4). La question était de savoir comment interpréter l'article 14 alinéa 1 de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC) ainsi que le concept qui a été élaboré par l'Office fédéral de la police (fedpol) pour les systèmes d'information JANUS et GEWA. La divergence principale portait sur le test 4 du concept; celui-ci statue que l'art. 14 al. 1 LOC n'est applicable que si les données ont été recueillies directement par fedpol ou par la Police judiciaire fédérale (PJF) et non pas par une autre autorité. Nous avions défendu le point de vue que les conditions stipulées dans l'article 14 al. 1 LOC devaient également être vérifiées dans le cas où les données n'étaient pas collectées directement. Le DFJP a cependant insisté pour maintenir ce test 4 en argumentant qu'il n'existait aucune disposition légale obligeant à informer ultérieurement les personnes concernées pour les données n'ayant pas été collectées directement par fedpol. C'est pourquoi il a fallu décider sur la base d'indices si cette thèse était fondée ou non. Le DFJP a tranché que l'article 14 al. 1 LOC n'est applicable que dans les cas où les données ont été collectées directement par fedpol. Cela implique que l'article 14 al. 1 LOC n'est jamais applicable au système d'information GEWA, puisqu'il n'existe dans ce cas aucune collecte directe de données de la part de fedpol. Le DFJP a en outre exprimé le vœu que fedpol fasse adapter les lois en conséquence lors d'une prochaine révision.

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

La protection des données est un élément important de l'évaluation menée par les experts européens dans le cadre de Schengen. Celle-ci se base sur un questionnaire et sur des inspections locales et concerne les autorités fédérale et cantonales de protection des données.

L'application de l'accord Schengen est subordonnée à une décision du Conseil de l'Union européenne. Celle-ci doit être prise à l'unanimité des Etats appliquant Schengen après évaluation de la capacité de la Suisse à mettre en oeuvre cet accord. L'évaluation est menée par des équipes composées d'experts du Conseil européen, de la Commission européenne et des Etats membres. Son but premier n'est pas de sanctionner, mais d'aider les nouveaux Etats à mettre leurs institutions en conformité avec les accords et l'acquis de Schengen. L'évaluation permet également de comparer les pratiques nationales et de les améliorer. Elle porte d'abord sur la coopération policière, la protection des données, le contrôle aux frontières extérieures, les visas, la coopération consulaire, puis sur le Système d'information Schengen (SIS) - une fois que celui-ci est opérationnel. L'évaluation se base sur un questionnaire et sur des inspections locales. Des évaluations ultérieures sont également menées auprès des pays qui sont déjà membres de Schengen.

L'évaluation de la protection des données porte sur les dispositions de l'accord régissant la protection des données et en particulier sur l'autorité de contrôle. Elle consiste en un questionnaire adressé aux autorités fédérale et cantonales de contrôle, puis en une visite auprès de celles-ci. Les bases légales régissant ces autorités sont analysées; on examine notamment leur indépendance, leurs compétences en matière d'investigations et de sanctions, ainsi que leur rôle de supervision, en particulier dans le contrôle du SIS et des services impliqués. Les droits des personnes concernées et la sécurité des données font également partie de l'évaluation. Les experts s'intéressent également aux contacts que les autorités de contrôle ont avec les autorités étrangères dans le cadre de la coopération internationale ainsi que les relations avec le public. Ils attachent une importance particulière à l'existence d'une politique de sensibilisation et de lignes de conduite pour les personnes concernées.

1.3.10 Accords de réadmission

L'Office fédéral des migrations travaille à l'élaboration de nombreux accords de réadmission dans lesquels des normes de protection des données sont introduites. Ces dernières pouvant varier, l'office prend contact avec nous pour avis.

Nous avons été consultés à de nombreuses reprises ces cinq dernières années au sujet d'accords de réadmission et de transit. Ces accords ont été conclus, d'une part, avec des Etats disposant d'une législation de protection des données adéquate comme les Etats de l'Union européenne et ceux ayant ratifié la Convention 108 du Conseil de l'Europe et, d'autre part, avec des Etats ne disposant pas de législation adéquate comme les Etats africains et asiatiques. Les principaux problèmes ont concerné la communication de données sensibles relatives à des procédures ou mesures administratives ou pénales. Ces problèmes sont détaillés dans notre 10ème Rapport d'activités 2002/2003 (ch. 3.2.2).

1.4 Santé

1.4.1 Avant-projet d'article constitutionnel et de loi fédérale relative à la recherche sur l'être humain

Nous approuvons la création d'une disposition constitutionnelle et d'une loi fédérale relative à la recherche sur l'être humain. L'avant-projet établit en tant que principe le consentement éclairé de la personne concernée pour chaque activité de recherche. Nous avons requis un certain nombre d'adaptations concernant le contenu des informations fournies au patient. Ces adaptations ont pour but d'améliorer la transparence du traitement de données pour les personnes concernées. En outre, nous avons exprimé nos préoccupations au sujet du projet de dissolution de la Commission fédérale d'experts du secret professionnel en matière de recherche médicale et critiqué la suppression de notre compétence en matière de surveillance et de recours.

Dans le cadre de la procédure de consultation, nous nous sommes prononcés sur l'avant-projet d'article constitutionnel et de loi fédérale relative à la recherche sur l'être humain (LRH). Ces dispositions règlent de manière globale l'ensemble de la recherche médicale sur l'être humain dans le domaine de la santé.

Nous avons vivement salué le fait qu'en plus des directives de l'Académie suisse des sciences médicales (ASSM), une réglementation à l'échelon suisse ait été entreprise concernant la recherche sur l'être humain et en particulier l'utilisation de données personnelles et de matériel biologique. Cette thématique, extrêmement importante pour les droits de la personnalité des donneurs, doit être réglementée clairement au niveau de la constitution et de la loi en tenant compte des principes du droit de la protection des données. Le «consentement éclairé» est un principe fondamental pour le traitement des données personnelles et du matériel biologique: il s'agit du consentement libre qui se fonde sur une information suffisante. Le consentement et l'information sont donc des conditions indispensables à toute activité de recherche.

Nous avons d'abord suggéré de mettre davantage l'accent sur la protection de la personnalité dans l'article consacré à l'objectif de la loi, ceci en référence au mandat constitutionnel nouvellement formulé de veiller à la protection de la dignité humaine et de la personnalité en tenant compte du principe de la liberté de la recherche. Le point de départ d'une réglementation légale de la recherche sur l'être humain doit être la garantie des droits des testeurs et des donneurs. Étant donné le caractère

sensible des données de recherche, qui sont en majeure partie des données sensibles au sens de la LPD, nous aurions en outre approuvé que l'on intègre dans la LRH des dispositions spécifiques en matière de protection des données dans le texte de loi. Le renvoi général à la LPD, contenu dans le projet de loi, nous a semblé trop global et trop peu précis.

La LRH érige au rang de principe dans le domaine de la recherche médicale le consentement donné après information suffisante et temps de réflexion adéquat. Ainsi, sans le consentement de la personne concernée, on ne doit pas pratiquer de recherche médicale à partir des données ou du matériel biologique de la personne concernée. Nous avons vivement approuvé ce principe car il tient compte de l'exigence de la transparence et de la justification du traitement des données. Nous avons par contre refusé dans ce contexte la possibilité prévue par la LRH d'une information trompeuse pour les projets de recherche lorsque celle-ci s'imposerait pour des raisons méthodiques. Une information trompeuse contredit fondamentalement le principe du consentement éclairé et n'est de ce fait absolument pas admissible. Par ailleurs, nous avons proposé que l'information englobe toujours le droit d'opposition et le droit de révocation – qu'il est possible de faire valoir en tout temps. Dans la mesure où la personne concernée fait usage de son droit de révocation, nous avons demandé que les données personnelles déjà collectées soient rendues anonymes ou effacées et que le matériel biologique soit détruit.

La LRH prévoit que les échantillons biologiques et les données personnelles peuvent aussi être exportés à l'étranger à des fins de recherche. Cette exportation comportant un risque accru d'atteinte à la personnalité pour les donneurs, nous avons approuvé le fait que les échantillons biologiques et les données ne puissent être exportées que sous une forme anonymisée ou pseudonymisée. De plus, nous avons demandé qu'en cas d'exportation, des règles adéquates de destruction et de restitution soient obligatoirement prévues pour les échantillons et les données. Dans le but d'améliorer la transparence, nous avons suggéré d'attirer l'attention de la personne concernée, lors de l'information, sur la possibilité de transférer ses données et son matériel biologique à l'étranger et sur son droit d'opposition. De même, les personnes qui participent à un projet de recherche doivent être informées des éventuelles obligations légales d'informer et de déclarer les résultats de la recherche, en dehors du contexte de la recherche (par ex. à des assurances) ainsi que sur les droits d'accès de tiers. C'est le seul moyen d'assurer, pour la personne concernée, une transparence suffisante sur ce qu'il advient de ses données et de ses échantillons biologiques.

Enfin, nous regrettons que la LRH projette de supprimer la Commission d'experts du secret professionnel en matière de recherche médicale. Cette commission, créée en vertu de l'art. 321bis CP et de l'art. 32 LPD, accomplit aujourd'hui une tâche importante: elle garantit le respect de la protection des données dans le domaine de la recherche médicale. Elle décide de la levée du secret médical lorsqu'il n'est pas (ou plus) possible d'obtenir le consentement des personnes concernées; elle arrête aussi les conditions et charges en cas de transmission de données à des tiers. Conformément à l'avant-projet, cette tâche devrait être dorénavant assumée par les commissions d'éthique compétentes. Nous avons exprimé nos sérieuses préoccupations à ce sujet. En effet, il est douteux que les intérêts de la protection des données soient suffisamment respectés lorsqu'il n'y aura plus de commission d'experts. Les tâches des commissions d'éthique portent en effet sur d'autres domaines et concernent en premier lieu l'autorisation de projets de recherche et leur appréciation sur le fond. De notre point de vue, la LRH tient trop peu compte de cet aspect. La LRH ne reprend notamment pas toutes les conditions qui doivent être remplies pour donner le droit de mener un projet de recherche, conformément à l'art. 321bis CP et à l'ordonnance concernant les autorisations de lever le secret professionnel (OALSP). Parallèlement à la suppression de la Commission d'experts du secret professionnel en matière de recherche médicale, les compétences du PFPDT quant à la surveillance et au recours dans le domaine de la recherche médicale ont aussi été réduites. Nous avons requis à ce propos que certaines de ces compétences (surveillance du respect des charges en matière de protection des données et information des patients par le corps médical; droit de recours contre les décisions des commissions d'éthique concernant la protection des données) soient conservées dans le domaine de la recherche en matière médicale et que les dispositions matérielles de la LRH soient modifiées en conséquence.

1.4.2 Traitement de données médicales dans le cadre d'un mandat (sous-traitance)

Les activités quotidiennes dans les hôpitaux devenant de plus en plus complexes du point de vue informatique, et ne cessent de soulever de nouvelles questions, notamment en ce qui concerne les données des systèmes d'imagerie qui nécessitent une mémoire importante. Contactés par une entreprise du secteur privé, nous avons examiné les conditions-cadres juridiques de la communication de données médicales par des hôpitaux privés à des tiers dans un but de sauvegarde des données et de délégation de gestion.

De nombreux hôpitaux ont recours au support de tiers pour la maintenance des données traitées au quotidien dans les hôpitaux. Au cours de l'année écoulée, nous avons été pour la première fois contactés par une entreprise désirant savoir si les données concernant les patients pouvaient être traitées en dehors de l'enceinte de l'hôpital, voire même à l'étranger.

Dans ce contexte, il convient en premier lieu de souligner qu'en raison du secret médical, le traitement des données des patients ne peut être confié à des tiers que si toutes les personnes concernées ont donné leur consentement. Si, en cas de sous-traitance, on désire exceptionnellement agir sans déclaration de consentement, des mesures d'ordre technique et organisationnel doivent garantir que les tiers mandatés n'ont pas accès aux données médicales. Dans la réalité, le traitement des données des patients montre qu'il s'agit là d'une tâche particulièrement difficile pour ce qui est de l'archivage de données et en particulier de la délégation de gestion. Si une solution n'est pas trouvée, la sous-traitance en matière de données de patients n'est ni conforme à la protection des données, ni au droit pénal.

En outre, si les données sont transférées à l'étranger, il faut vérifier si le pays destinataire possède des dispositions de protection des données équivalentes aux nôtres. Si tel n'est pas le cas, des mesures de précaution adéquates s'imposent (pour plus de précisions, consulter notre site web www.edoeb.admin.ch, sous la rubrique Thèmes - Protection des données - Transmission à l'étranger). En outre, nous avons de sérieux doutes à l'égard d'un traitement de données de patients sur le territoire national des Etats-Unis, étant donné l'évolution récente du droit américain. Face à un tel projet, il ne faudrait en aucun cas omettre de contrôler si et comment on peut empêcher un accès non souhaité, sur la base de la législation anti-terrorisme, à des données suisses concernant des patients; la seule référence aux principes du Safe Harbour Agreement ne change rien à la situation.

1.4.3 Communication par les hôpitaux de données de diagnostic aux assureurs

La codification permet de fournir une multitude d'informations sous une forme succincte. Les diagnostics médicaux en sont un exemple. Les diagnostics sont codés par groupes de cas (Diagnosis Related Groups, DRG). L'utilisation des DRG a suscité quelques demandes de particuliers. Il n'existe actuellement aucune base légale qui permette aux prestataires de communiquer systématiquement des données médicales détaillées aux assureurs.

Il est prévu à l'avenir d'utiliser des forfaits de coûts par cas liés au diagnostic pour l'indemnisation des séjours dans le domaine stationnaire somatique aigu. A cette fin, une banque de données nationale sera créée dans une première étape. Dans une deuxième étape, les prestations des hôpitaux seront remboursées sur la base des forfaits de coûts par cas qui ont été calculés. Les deux étapes requièrent des diagnostics détaillés.

Les exigences de la législation sur la protection des données sont différentes pour les deux étapes. La banque de données doit impérativement être créée à partir de données anonymisées. Dans la deuxième étape, à savoir l'application proprement dite du système DRG, les données se réfèrent à une personne. Il s'agit d'une communication systématique par le prestataire de services de données médicales très détaillées à l'assureur. Une telle communication n'est pas admissible selon la législation actuellement en vigueur. S'il est prévu à l'avenir d'utiliser les forfaits de coûts par cas comme base pour le décompte des prestations, il y a lieu de créer d'abord les bases légales nécessaires.

1.4.4 La protection des données dans un cabinet médical

Dans un cabinet médical moderne, l'infrastructure informatique et surtout les données relatives aux patients doivent être protégées de manière pratique et efficace. Des questions qui nous ont été adressées ainsi que certaines réactions de médecins entendues lors de conférences dans le domaine de la santé publique nous montrent qu'il existe une certaine incertitude quant aux mesures apparaissant judicieuses. C'est pourquoi nous avons décidé de publier un catalogue décrivant les mesures de protection minimales.

De manière simplifiée, on peut subdiviser un cabinet médical en quatre secteurs:

Le premier secteur comprend le serveur avec les fonctions centrales et les données des patients. L'objectif dans ce secteur est d'éviter tout accès non autorisé au système par une authentification efficace par mot de passe et de prévenir les pertes de données par des stratégies de sauvegarde appropriées.

Le deuxième secteur englobe l'ensemble de l'infrastructure du cabinet médical. La majorité des équipements sont reliés entre eux par un réseau local. Il s'agit ici de veiller à ne raccorder au réseau que les équipements vraiment nécessaires pour éviter que ce dernier inclue des équipements qui échappent à tout contrôle. Les périphériques doivent être configurés de manière à ce que des tiers n'y aient pas accès et placés de sorte à ce qu'une personne non autorisée ne puisse entrevoir des informations, par exemple à l'écran.

Le secteur suivant comprend le bureau privé du médecin qui peut par exemple être situé à son domicile privé. Une éventuelle transmission de données de patients par le biais d'Internet doit impérativement être cryptée. Une meilleure manière de procéder consiste à copier les données sur l'ordinateur portable en les cryptant avant de quitter le cabinet.

Le quatrième secteur comprend les réseaux publics, en particulier Internet. En principe, les systèmes utilisés dans le cabinet médical doivent être déconnectés des réseaux publics. Aussi bien les travaux de maintenance des équipements du cabinet que l'accès à Internet depuis les équipements situés dans le cabinet doivent s'effectuer de manière contrôlée. Cela signifie que toutes les transmissions de données entre le cabinet médical et les réseaux publics doivent transiter par un système pare-feu. On évitera notamment de télécharger des fichiers depuis Internet sur les systèmes du cabinet médical. La maintenance à distance ne devrait pas s'effectuer à travers une connexion Internet, mais moyennant des modems de télémaintenance dédiés.

Malgré toutes les mesures techniques prises, il importe de ne pas oublier certaines précautions fondamentales: les données des patients ne doivent être traitées que lorsque cela est vraiment nécessaire et toujours avec la circonspection de rigueur. Le médecin doit en tout temps connaître la situation actuelle de l'informatique de son cabinet.

Vous trouverez des exigences plus détaillées sur notre site web ainsi que sur un cédérom de la Société suisse de médecine générale SSMG (www.ssmg.ch).

1.4.5 Surveillance de l'application des charges délivrées par la Commission d'experts dans le domaine de la recherche médicale

Dans le domaine de la recherche médicale, on parle souvent de «données anonymisées». Dans la majorité des cas cependant, il s'agit en fait de données «pseudonymisées». On entend par données anonymisées des données pour lesquelles il est impossible ou extrêmement difficile d'identifier la personne qu'elles concernent. Dans le cas de données pseudonymisées par contre, une telle identification est possible. Nous avons en outre encore dû constater cette année que la poursuite de nos contrôles dans le domaine de la recherche médicale est nécessaire.

Nous avons constaté que la notion de «données anonymisées» n'était pas toujours appliquée correctement dans le domaine de la recherche médicale. Beaucoup de projets de recherche utilisent des données pseudonymisées. On parle de pseudonymisation dans les cas où les données identifiantes sont séparées des autres données. Les deux blocs de données peuvent être mis en relation grâce à un numéro unique qui doit être présent aussi bien dans les données identifiantes que dans les autres données. C'est par l'intermédiaire de ce numéro que l'on peut à nouveau réunir les deux blocs de données; c'est ce qu'on appelle la „dépseudonymisation". Il arrive que l'on constate au cours d'un projet de recherche que l'on a encore besoin d'autres informations. Si les données ont été pseudonymisées, il sera possible dans un tel cas de déterminer l'identité de la personne concernée et donc de collecter les données complémentaires. Le processus de la dépseudonymisation doit cependant impérativement être retraçable. Le chercheur ne doit pas être autorisé à procéder lui-même à cette dépseudonymisation (séparation des fonctions). On parle par contre de données anonymisées lorsque l'effort, le temps et les coûts liés à une mise en relation de ces données avec une personne déterminée ou déterminable seraient démesurément élevés.

Cette année, nous avons également procédé à des contrôles dans le domaine de la recherche médicale afin d'établir comment étaient appliquées les charges délivrées par la commission d'experts (cf. également notre 13ème rapport d'activités 2005/2006, ch. 4.1.2). Dans la majorité des cas, nous avons pu constater que l'accès aux systèmes d'information était bien protégé, de sorte que nous n'avons pas dû émettre de critiques. Dans un cas, nous avons dû néanmoins indiquer qu'il fallait clairement séparer les données actuelles des données archivées et que tout accès à des données non anonymisées devait être organisé de manière à ce qu'il puisse en tout temps être reconstitué. Un autre cas concerne un hôpital dans lequel nous avons constaté que les projets de recherche étaient surtout effectués avec des données papier issues des archives centrales. On n'a cependant pas pu nous indiquer s'il était également possible que des projets de recherche soient effectués sur la base de fichiers électroniques car les données correspondantes faisaient défaut. Nous devons malheureusement constater un manque de transparence dans ce domaine, ce qui rend très difficile une application satisfaisante des exigences de la protection des données.

Nous continuerons à procéder à des contrôles dans le domaine de la recherche médicale.

1.5 Assurances

1.5.1 Questions de protection des données liées à l'introduction de la carte d'assuré

L'élaboration des bases techniques et du projet d'ordonnance ont été les grandes étapes du projet «carte d'assuré» dans l'exercice écoulé. L'introduction de la carte d'assuré représente un événement fondamental pour la santé publique. C'est pourquoi il est également essentiel que les exigences de base de la protection des données soient rigoureusement respectées. Des erreurs qui seraient commises dans la phase initiale d'introduction de la carte-santé ne pourront être corrigées après coup que moyennant des efforts très importants aussi bien au niveau organisationnel que financier.

Dans sa déclaration relative au projet d'ordonnance sur la carte d'assuré, l'Office fédéral de la santé publique (OFSP) relève que l'article 42a alinéa 4 de la loi fédérale sur l'assurance-maladie (LAMal) doit être considéré comme un premier pas vers une carte-santé. Ce premier pas implique qu'il est prévu d'enregistrer sur la carte non seulement des données purement administratives, mais également des informations mé-

dicales concernant la personne assurée (cf. notre 13ème rapport d'activités 2005/2006, ch. 5.1.1). Le législateur exige que cet enregistrement soit impérativement soumis au consentement de la personne assurée. Pour que la personne assurée puisse donner son consentement, elle doit cependant recevoir une information claire, compréhensible et complète sur le traitement des données la concernant.

Le projet d'ordonnance inclut une énumération exhaustive des données: données relatives au groupe sanguin et à la transfusion; données relatives au système immunitaire; données relatives à la transplantation; allergies; maladies et séquelles d'accidents; inscription supplémentaire dans des cas médicalement fondés; médication; une ou plusieurs adresses de personnes à avertir en cas d'urgence; mention de l'existence de directives anticipées du patient. Ces données devraient être enregistrées sur la carte d'assuré dans le but d'améliorer l'efficacité, la sécurité et la qualité du traitement médical.

Ont accès à ces données les médecins, pharmaciens, médecins-dentistes, chiropraticiens, sages-femmes, physiothérapeutes, ergothérapeutes, le personnel soignant spécialisé, les orthophonistes et les diététiciens. L'enregistrement des données et leur consultation ne peuvent être effectués qu'avec le consentement de la personne assurée. Quant à l'information du patient, le projet d'ordonnance prévoit qu'elle sera faite par les prestataires mentionnés ci-dessus.

Cette extension de l'usage d'une carte administrative utilisée pour la facturation des prestations selon la LAMal à une carte contenant des données de santé a des conséquences sur les droits de la personnalité des assurés et doit donc être effectuée de manière conforme aux exigences de la protection des données.

Ainsi, il convient en premier lieu de s'assurer que les données conviennent pour le but prévu par le législateur. Les prises de position que nous avons reçues de la part des prestataires nous montrent cependant – même en interprétant très largement – que ceci n'est pas le cas. Au contraire: de l'avis de la Fédération des médecins suisses, certaines informations telles que les données de groupe sanguin et de transfusion sanguine pourraient à la rigueur procurer au patient un sentiment de sécurité. Quant aux informations concernant les maladies et la médication, elles posent problème car aucune garantie ne peut être donnée qu'elles soient toujours complètes et mises à jour. L'association suisse des hôpitaux H+ a également publié une déclaration très claire sur l'utilité des données de santé enregistrées sur la carte santé. Elle considère le fait d'utiliser la même carte comme carte d'assuré et comme carte santé comme un choix malencontreux.

Deuxièmement, il y a lieu de veiller à ce que le patient soit clairement informé des conséquences de son consentement et qu'il en mesure la portée. Etant donné que ces informations peuvent renseigner sur l'état de santé du patient et d'autres événements qui ont un caractère délicat ou intime, cette information doit être particulièrement complète et claire. Le patient doit savoir qui utilise ses données et à quelles fins. Ce n'est qu'ainsi qu'il sera en mesure de peser le pour et le contre de son consentement. La question se pose cependant de savoir qui lui transmettra ces informations. La majorité des prestataires de services et de leurs représentants nient l'utilité d'enregistrer des données médicales sur la carte. Ils ne pourraient ainsi pas obtenir un consentement du patient, à moins de feindre un motif. Ceci ne peut cependant pas être le but de la carte d'assuré.

Finalement, les conditions de base pour le traitement des données de santé doivent être remplies. Il n'existe pas de réglementation suffisante sur ce qui sera fait avec ces données dans la pratique et qui assumera quelles responsabilités pour les différentes données. Selon le commentaire concernant le projet d'ordonnance, la personne assurée peut choisir dans la liste les catégories de données qu'elle désire voir enregistrées sur la carte. La question reste ouverte si cela sera finalement le désir du patient lié au consentement du prestataire qui déterminera quelles données médicales seront enregistrées sur la carte ou plutôt l'inverse, c'est-à-dire la proposition du prestataire acceptée par le patient.

Si l'une de ces trois conditions n'est pas remplie, il est permis d'émettre de très forts doutes sur la licéité de la carte d'assuré telle que celle-ci est prévue.

Beaucoup de questions importantes relevant de la protection des données n'ont donc pas encore trouvé de réponse. Les prestataires n'accueillent pas favorablement le traitement des données de santé. C'est pourquoi nous avons, tant dans le cadre du groupe de spécialistes tenu d'élaborer les normes techniques que de nos prises de position sur le projet d'ordonnance, demandé à l'OFSP de renoncer à enregistrer des données médicales sur cette carte. Le risque est trop élevé que des patients consentent expressément à un traitement de leurs données de santé sans avoir été informés suffisamment sur le but du traitement.

1.5.2 Transparence du traitement des données dans la procédure de l'assurance- accidents

Nous avons été consultés au sujet de la première étape de la révision de loi fédérale sur l'assurance-accidents. Du point de vue de la protection des données, il convient de veiller à ce que la transparence du traitement des données dans le domaine de l'assurance-accidents ne se détériore pas. Tel serait le cas si la collecte des informations par l'assurance-accidents avait désormais lieu sans le consentement de la personne concernée.

La loi sur la partie générale du droit des assurances sociales (LPGA) est entrée en vigueur en 2003. Ce texte de loi a posé une règle, valable pour l'ensemble du domaine des assurances sociales: l'assureur social doit recevoir l'autorisation des assurés (qui désirent bénéficier des prestations) pour collecter des renseignements (art. 28 al. 3 LPGA). Or, le projet de révision de la loi fédérale sur l'assurance-accidents (LAA) prévoit désormais de ne plus appliquer cette règle dans le domaine de l'assurance-accidents. Dans le cadre de la consultation, nous nous sommes prononcés contre la mise en œuvre de ce projet.

L'autorisation - prévue par la LPGA - permettant la transmission de renseignements revêt une importance certaine. Si cette autorisation n'est pas donnée, le refus de collaborer peut avoir des conséquences défavorables pour l'assuré. Mais en même temps, l'assuré tire aussi un avantage de l'obligation de donner son autorisation: ce faisant, il reçoit des informations sûres sur les circonstances entourant la collecte d'informations et leurs destinataires; ce n'est qu'ainsi que l'assuré peut avoir une perception quelque peu transparente du traitement de données le concernant et entrepris par l'assureur.

Même s'il convient d'admettre que les assurances-accidents ont comparativement besoin de beaucoup d'informations pour traiter les dossiers des cas d'accidents, il faut conserver le système en place imposant la déclaration d'autorisation. Le droit à un traitement transparent des données ne doit pas être affaibli sans motif impératif.

1.6 Secteur du travail

1.6.1 Contrôle auprès de la société ALDI SUISSE SA

Au cours de l'année 2006, nous avons procédé à un contrôle approfondi en matière de protection des données dans une succursale du groupe ALDI Suisse. Ce contrôle a porté principalement sur la surveillance vidéo dans le commerce de détail. Le but principal d'une telle surveillance – la protection contre le vol et les agressions – a été mis en rapport avec la proportionnalité de la mesure et son impact sur les droits de la personnalité. Après avoir procédé à une appréciation nuancée de l'ensemble de la situation, nous avons dû recommander que des adaptations soient faites en matière de protection des données. En plus de certaines améliorations, ALDI devra en particulier positionner les caméras situées dans le secteur des caisses de manière à ce que la surveillance des collaborateurs ne soit pas possible. ALDI s'est en outre engagé à utiliser des technologies respectueuses de la protection des données (techniques de floutage).

Notre société de consommation manifeste un vif intérêt à examiner de près le comportement de la clientèle. En 2005, nous avions – en notre qualité d'autorité de surveillance pour la protection des données – contrôlé si les traitements de données effectués par Migros et Coop dans le cadre de leurs programmes M-CUMULUS et Supercard étaient conformes à la législation en matière de protection des données (cf. notre 13ème rapport d'activités 2005/2006, ch. 7.1 et 7.2). En 2006, nous avons procédé auprès de la société ALDI SUISSE SA (désignée ci-après par ALDI) à un contrôle de l'installation de vidéosurveillance afin de vérifier sa conformité avec la législation en matière de protection des données.

ALDI a récemment ouvert plusieurs succursales en Suisse. Comme tous les détaillants, ALDI se voit confronté au problème des vols et des hold-up. L'installation d'un système de vidéosurveillance constitue – en plus des mesures organisationnelles et des dispositions prises au niveau de la construction – une mesure permettant de lutter contre ces menaces. Les succursales d'ALDI sont toutes construites selon un modèle standard. L'exploitation d'un système de vidéosurveillance touche toujours une multitude de personnes (collaborateurs, fournisseurs, clients). Le contrôle que nous avons effectué s'inscrivait surtout dans le contexte de la problématique générale

de la vidéosurveillance dans le commerce de détail pendant les heures de travail et les heures d'ouverture. Les constatations faites ainsi que les recommandations qui en découlent doivent inciter d'autres exploitants de systèmes de vidéosurveillance à entreprendre les corrections nécessaires dans les cas où leurs systèmes ne seraient pas entièrement conformes.

En surveillant la marchandise et en permettant d'élucider les éventuels vols et agressions, une installation de vidéosurveillance poursuit des objectifs légitimes. Avant l'installation d'un tel système, il est néanmoins nécessaire d'examiner s'il existe d'autres mesures efficaces qui porteraient moins atteinte aux droits de la personnalité des personnes concernées. Si l'installation d'un système de vidéosurveillance s'impose, le concept de mise en œuvre doit non seulement tenir compte de l'objectif visé mais également des droits à la personnalité des clients et des collaborateurs de l'entreprise. Ceci concerne notamment la surveillance du secteur dans lequel se trouvent les caisses ainsi que la surveillance de l'espace de vente. Toutes les caméras doivent être orientées de manière à ce que n'entrent dans leur champ de vision que les objets dont la surveillance est envisagée (cf. le feuillet thématique «Vidéosurveillance effectuée par des personnes privées» sur notre site web). Cela signifie que les caméras placées dans l'entrée doivent avoir un champ de vision limité qui ne couvre pas les secteurs extérieurs où circulent les passants. Des panneaux suffisamment grands et bien visibles doivent être placés dans l'entrée à hauteur des yeux pour signaler que des caméras vidéo sont installées à cet endroit et que celles-ci enregistrent les mouvements de toutes les personnes depuis leur entrée dans la succursale jusqu'à leur sortie. Pour la vidéosurveillance de l'espace de vente proprement dit, les caméras doivent être orientées de manière à ce qu'elles surveillent en priorité les marchandises de valeur qui pourraient facilement être dissimulées par un client dans une poche, une veste ou un sac. Bien qu'ALDI mentionne expressément dans ses directives d'utilisation que les caméras ne peuvent être installées dans le but de surveiller le personnel, notre contrôle a révélé que les caméras situées dans le secteur des caisses couvraient dans leur champ de vision également les personnes travaillant aux caisses. Nous ne voulons en aucune manière insinuer qu'ALDI avait l'intention de surveiller son personnel, mais il est de notre devoir d'exclure d'emblée toute possibilité d'une telle surveillance. Comme mesure de protection de la santé, le droit du travail interdit d'utiliser des systèmes de surveillance permettant d'observer le comportement des collaborateurs à leur place de travail. Si de tels systèmes s'avèrent nécessaires pour d'autres raisons, ils doivent être conçus et installés de manière à ne pas entraver la santé et la liberté de mouvement des employés.

Chez ALDI, les enregistrements vidéo ne sont pas accessibles à tous les collaborateurs. Cet accès est réglementé de manière très stricte: en cas de soupçon fondé, seules les personnes autorisées peuvent, après authentification par mot de passe, visionner ces enregistrements à des fins de contrôle. Nous avons dans le cadre de notre contrôle souligné le fait que les technologies respectueuses de la protection des données (techniques de floutage) deviendront prochainement la norme pour les installations de vidéosurveillance. Ces technologies présentent l'avantage que les personnes surveillées ne sont pas d'emblée identifiables; ce n'est qu'en cas de soupçon fondé qu'un collaborateur autorisé pourra à nouveau rendre visible une personne en supprimant le floutage. De plus, l'installation de technologies respectueuses de la protection des données permet de laisser les écrans du système de surveillance allumés en permanence. Nous avons recommandé à ALDI de mettre en œuvre de telles technologies au plus tard jusqu'à fin 2008. Il nous tient à cœur que les installations de vidéosurveillance dans le domaine tertiaire n'utilisent dorénavant plus que des technologies respectueuses de la protection des données.

ALDI SUISSE SA a accepté toutes les recommandations que le PFPDT a faites dans son rapport final (vous trouverez ce dernier sur notre site web www.edoeb.admin.ch). A part certaines adaptations au niveau du positionnement des caméras, ALDI s'est notamment engagé à modifier au plus tard fin mars 2007 l'orientation des caméras situées dans le secteur des caisses, de manière à ce que la possibilité de surveiller les collaborateurs travaillant à une caisse soit exclue. ALDI s'est également engagé à mettre en œuvre des technologies respectueuses de la protection des données (techniques de floutage) dès que celles-ci pourront être livrées par le fournisseur du système de vidéosurveillance, mais en tout cas d'ici fin 2008.

1.6.2 Conditions posées à la demande d'extraits du casier judiciaire par une entreprise

Une entreprise de transport se procure les extraits de casier judiciaire de ses employés afin de protéger ses propres intérêts en matière de sécurité et de satisfaire aux normes internationales. Nous avons examiné cette mesure sous l'angle de sa conformité avec la protection des données et sommes parvenus à la conclusion qu'elle était en principe justifiée. En même temps, nous avons attiré l'attention de l'entreprise sur le fait qu'une telle mesure représentait une atteinte grave à la personnalité des employés et qu'elle devait donc reposer sur deux principes: celui de la proportionnalité et celui de la transparence.

Suite à diverses demandes émanant des employés d'une entreprise de transport, nous avons examiné la question de savoir dans quelles circonstances un employeur a le droit de se procurer les extraits du casier judiciaire de ses employés. Dans le cas d'espèce, l'entreprise de transport justifiait la recherche des extraits du casier judiciaire par la valeur de la marchandise transportée et par l'augmentation des pertes de marchandises, mais elle invoquait aussi les normes internationales en matière de sécurité des marchandises ainsi que l'amélioration de sa compétitivité. La marchandise qu'il s'agit de protéger comporte entre autres des produits dangereux et des biens de grande valeur. Selon les informations fournies par l'entreprise, la demande de l'extrait du casier judiciaire ne constitue qu'une mesure de sécurité parmi d'autres devant permettre de garantir l'intégrité et la conservation des biens et marchandises transbordées.

Nous avons tout d'abord établi un certain nombre de points à propos du problème ici posé: en vertu de la loi sur la protection des données, tout traitement de données personnelles doit être justifié. La loi considère comme motif justificatif le consentement de la personne concernée, la présence d'un intérêt prépondérant ou une loi. Dans le cas présent, ni une loi ni le consentement de la personne concernée n'entrent en ligne de compte comme motif justificatif; nous avons donc examiné si un intérêt prépondérant privé ou public de l'entreprise pouvait justifier une demande d'extrait du casier judiciaire de ses employés.

Bien que l'atteinte à la personnalité de la personne concernée puisse être grave, nous sommes partis du principe que les intérêts de la sécurité de l'entreprise étaient dans le cas d'espèce prépondérants. Il convient de souligner à cet égard que le casier judiciaire renferme des données sensibles au sens de la loi sur la protection des

données, à savoir celles qui concernent les poursuites et les sanctions pénales. La consultation de l'extrait du casier judiciaire par des tiers constitue une atteinte grave à la personnalité de la personne concernée. Elle nécessite, outre un motif justificatif, une nécessité ainsi qu'un rapport raisonnable entre le motif du traitement et l'atteinte à la personnalité.

Il convient donc tout d'abord d'examiner si d'autres mesures portant moins atteinte à la personnalité des employés ne permettraient pas aussi d'atteindre l'objectif visé. A cet effet, l'entreprise a établi une liste de mesures de sécurité comprenant la gestion de l'accès, les contrôles des véhicules et des personnes, la surveillance des rampes et la sécurité dans l'enceinte de l'entreprise. Toutefois, une protection absolue des biens est impossible à atteindre. Certaines mesures de sécurité - par exemple les contrôles des personnes -constituent en partie une atteinte grave à la personnalité des employés, de sorte qu'elles ne peuvent être appliquées de manière systématique, mais uniquement sur la base de contrôles effectués au hasard. D'autres mesures peuvent éventuellement être contournées par les employés. Dans cette optique et compte tenu de la valeur des biens à protéger, nous avons établi que le fait de se procurer un extrait du casier judiciaire devait être considéré comme un complément non seulement utile, mais aussi nécessaire au concept de sécurité.

Il semble y avoir également une relation raisonnable entre le but du traitement et l'atteinte à la personnalité. Cela dit, la demande d'extrait du casier judiciaire ne doit concerner que les catégories de collaborateurs qui ont, d'une façon ou d'une autre (c'est-à-dire directement, ou par le biais de moyens informatiques ou de documents), accès aux marchandises.

En outre, il convient de veiller à ce que ces extraits du casier judiciaire des employés ne soient consultés que par un nombre minimal de personnes. L'entreprise nous a informés que le service du personnel effectuait un premier triage après réception des extraits du casier judiciaire. Nous avons établi que non pas l'ensemble du service du personnel, mais uniquement un nombre restreint d'employés de ce service devait avoir accès aux extraits du casier judiciaire. Dans l'idéal, ce triage devrait être effectué directement par le chef du personnel, sans que d'autres collaborateurs ne soient impliqués. En outre, il faut attirer l'attention des personnes participant au processus d'évaluation sur leurs devoirs de confidentialité. L'extrait du casier judiciaire doit être détruit lorsque le but du traitement est atteint. Les données saisies ne doivent pas être accessibles à des tiers non autorisés.

Enfin, nous avons également examiné la question de savoir si la mesure en question était mise en œuvre avec suffisamment de transparence à l'égard des employés. Plus le traitement des données a un impact important sur les droits de la personnalité, plus

les exigences concernant la transparence et le principe de la bonne foi sont élevées. Dans le cas d'espèce, les employés étaient informés par un formulaire de consentement. Nous avons donc considéré que ce principe était respecté. Il convient bien entendu de garantir le droit à l'information pour la personne concernée.

1.6.3. L'engagement de «clients testeurs» dans les entreprises de transport

Les entreprises de transport qui utilisent des «clients testeurs» afin d'évaluer leur personnel de manière dissimulée doivent veiller à ce que la protection de la personnalité des employés concernés soit garantie. Ainsi, une grande partie du temps de travail doit demeurer non surveillé. Par ailleurs, les employés doivent avoir la possibilité de prendre position sur les évaluations les concernant et en cas de litige, de rencontrer les clients testeurs en question.

Un syndicat nous a prié d'examiner sous l'angle de la protection des données la pratique d'une entreprise de transport qui soumettait ses chauffeurs à des évaluations effectuées par des clients testeurs anonymes. Il faisait essentiellement valoir que le traitement en question ne visait pas, comme on l'avait officiellement annoncé, le maintien et l'amélioration de la qualité, mais qu'il avait pour but la surveillance et l'évaluation des chauffeurs. Il mentionnait en outre que ceux-ci n'étaient pas informés du moment de ces actions et qu'en conséquence, ils se sentaient sous surveillance permanente. Enfin, le syndicat contestait le fait que les chauffeurs n'avaient pas accès aux données les concernant. Le syndicat en arrivait donc à la conclusion que les données portant sur l'évaluation des chauffeurs étaient collectées de manière contraire à la loi sur la protection des données.

Pour sa part, l'entreprise de transport assurait que ces actions de surveillance anonymes avaient comme but premier le maintien et l'amélioration de la qualité, du point de vue de la clientèle. Elle indiquait en outre que les données constituant les appréciations n'étaient utilisées que dans certaines régions comme base de discussion et comme référence lors des entretiens annuels avec les collaborateurs.

En premier lieu, il convient de retenir que le maintien et l'amélioration de la qualité ainsi que l'appréciation du collaborateur – en tant que buts indiqués par l'entreprise de transport - peuvent être considérés comme des intérêts prépondérants à ceux des personnes examinées à la protection de leur personnalité. Il y a donc là un motif justificatif pour le traitement de données au sens défini par la LPD. Mais pour être considéré comme conforme à la protection des données, le traitement des données doit également être proportionné.

Le fait de procéder à une évaluation dissimulée par le biais de clients testeurs constitue concrètement, selon la manière dont cette évaluation est organisée et selon son contenu, une atteinte plus ou moins grave aux droits de la personnalité des personnes concernées. Nous avons conclu qu'il s'agit ici d'un profil de la personnalité. Nous avons donc souligné que l'évaluation dissimulée menée par des clients testeurs est proportionnée et ne peut donc être effectuée que si d'autres mesures affectant moins la personnalité s'avèrent insuffisantes ou irréalisables. Si tel est le cas, l'évaluation dissimulée peut être effectuée, mais uniquement durant une période limitée. Le traitement doit alors se limiter aux seules données absolument nécessaires au but poursuivi.

Nous avons examiné le questionnaire remis aux clients testeurs et l'avons jugé nécessaire et apte à évaluer les chauffeurs de façon appropriée. Nous avons toutefois constaté que certaines questions figurant sur la feuille d'évaluation pouvaient générer des jugements de valeur subjectifs. Or, l'exactitude des données ne peut se référer qu'à des faits qui peuvent être constaté objectivement. Il est par contre difficile de classer des jugements de valeur subjectifs comme étant justes ou faux. Les données personnelles sont justes lorsqu'elles reflètent de manière adéquate les circonstances et les faits relatifs à une personne. La loi sur la protection des données prévoit, pour la personne traitant des données personnelles, l'obligation de s'assurer que celles-ci sont correctes. Elle prévoit également un droit de rectification. La personne concernée peut en effet subir une atteinte importante à sa personnalité par le traitement de données inexactes, par exemple lorsqu'une entreprise congédie un employé sur la base de données d'évaluation inexactes.

Dans le cas présent, le fait que les clients testeurs puissent demeurer anonymes parle contre l'objectivité des données d'évaluation, respectivement contre leur exactitude. Certes, l'anonymat les protège contre les menaces par exemple, mais les met en même temps en mesure d'exprimer des affirmations fausses sur un chauffeur à partir d'une position totalement protégée. En revanche, la personne évaluée se trouve dans une position non protégée, vulnérable. Certes, l'employé mis en cause peut éventuellement faire valoir un droit de rectification auprès de l'entreprise, mais une confrontation loyale et transparente avec son propre évaluateur, en l'occurrence le client testeur, n'est pas possible. Ainsi, il ne sera pas possible non plus de poursuivre un client testeur pour calomnie ou diffamation avec une quelconque chance de succès. L'égalité de traitement entre client testeur et employé n'est, en raison du déséquilibre des forces, manifestement pas garantie.

Les clients testeurs reçoivent une formation trop brève, ce qui constitue un autre problème quant à l'objectivité des données d'évaluation. De même, le contrat d'engagement ne fait pas, ou pas suffisamment, mention du problème de la protection des données, et particulièrement de la nécessité de disposer de données exactes et objectives.

En outre, nous avons critiqué le fait que les évaluations ont lieu durant toute l'année. Le chauffeur ne connaît ni le client testeur, ni la date exacte des évaluations. Il peut ainsi se sentir toute l'année sous pression et surveillance constantes. Cette pression peut engendrer des problèmes de santé. En l'occurrence il s'agit en premier lieu d'une surveillance, en principe admissible, de la prestation de l'employé – et non pas de la surveillance du comportement de celui-ci, qui est quant à elle interdite –; en outre, la surveillance n'est pas effectuée par un système de surveillance au sens strict du terme. Néanmoins, la problématique de la protection de la santé et de la personnalité est manifeste. Bien que ladite surveillance puisse être qualifiée d'appropriée pour remplir les objectifs poursuivis, il n'est pas nécessaire de l'étaler sur un tel laps de temps, et il n'existe pas non plus une proportion raisonnable entre une surveillance qui dure toute l'année et l'atteinte à la personnalité.

La collecte de données ainsi que tout autre traitement de données doivent être reconnaissables pour la personne concernée. Celle-ci doit donc pouvoir les déduire des circonstances ou être informée en conséquence. Sur la base des documents fournis, nous avons conclu que l'information avait bien eu lieu, tant sur les buts de la surveillance, sur les données traitées que sur la durée de la période de surveillance. Toutefois ni le droit d'accès, ni l'organisme chargé de donner ces informations n'étaient mentionnés. De même, il n'existait aucune information sur les périodes de contrôle sélectionnées.

Après avoir examiné l'engagement de clients testeurs, nous avons soumis quelques propositions d'amélioration à l'entreprise de transport. Nous lui avons aussi suggéré de supprimer du questionnaire d'évaluation les questions dont la réponse dépendait de façon importante de la perception subjective du client testeur. Nous avons également rappelé à l'entreprise que le principe de l'exactitude des données était une exigence fondamentale qu'un maître de fichier se devait de respecter.

Le cas échéant, afin de renforcer la position de l'employé ayant fait l'objet de l'évaluation, il convient de permettre une confrontation entre le chauffeur et le client testeur. Les chauffeurs tout comme les clients testeurs doivent en être informés au préalable. Nous avons requis de l'entreprise de transport qu'elle veille à ce que le chauffeur puisse immédiatement faire valoir son droit de réponse. Cela suppose que l'on n'attende pas des semaines pour l'informer d'une évaluation négative, mais qu'il la reçoive au plus tard deux jours après son établissement.

En regard du principe de la proportionnalité, nous avons formulé quelques propositions d'amélioration: occasionnelles, les évaluations dissimulées devraient en règle générale être annoncées à l'avance. Afin de tenir compte des intérêts de l'employeur, notamment de l'efficacité de l'évaluation, il n'est pas incompatible avec la protection de la personnalité de n'informer les employés que de la période d'évaluation choisie. Il convient en tout cas de veiller à ce que l'employé puisse avec certitude considérer qu'une partie essentielle de son temps de travail demeure exclue de l'évaluation. Une solution consisterait par exemple à effectuer plusieurs contrôles et à réduire la durée des périodes de contrôle à un total de quatre mois par an, en informant à l'avance les personnes concernées des périodes de contrôle choisies.

En outre, nous avons noté que les données de l'évaluation constituaient un profil de la personnalité et ne pouvaient en général être consultées que par les supérieurs hiérarchiques. Dans le cas présent, ce sont par contre les employés du service du personnel qui saisissent dans le système les données fournies par les clients testeurs. Nous avons prié l'entreprise de transport de confier l'accès aux données ainsi que leur saisie à des personnes de confiance à l'intérieur de l'entreprise, spécialement formées pour cela. En outre, le nombre de ces personnes doit demeurer restreint. Du point de vue technique, il convient de veiller à ce que les données saisies ne soient pas accessibles à des tiers non autorisés.

Relevons également que les clients testeurs doivent tout spécialement veiller à la confidentialité des questionnaires; il faut également prévoir par contrat l'obligation de détruire immédiatement d'éventuelles copies après remise de l'original à l'entreprise de transport. La transmission des questionnaires doit être accompagnée de mesures de protection appropriées. Si cette transmission a par exemple lieu par Internet, il convient d'envisager un cryptage des données.

Chaque employé de l'entreprise de transport doit pouvoir demander des renseignements sur les données traitées le concernant. Ce droit lui permet de contrôler les données dans le but de vérifier le respect des principes de la protection des données (licéité de la collecte, bonne foi, exactitude des données et proportionnalité) et le cas échéant d'en exiger la mise en oeuvre.

1.6.4 Révision de l'ordonnance sur la protection des données personnelles dans l'administration fédérale

Dans notre prise de position relative à l'ordonnance sur la protection des données personnelles dans l'administration fédérale, nous avons pour l'essentiel conclu qu'il fallait encore créer dans la loi sur le personnel de la Confédération les bases légales nécessaires à l'ordonnance. Nous avons également demandé que les réglementations concernant les autorisations d'accès soient plus restrictives. A la suite d'une séance avec différents offices fédéraux, nous avons constaté après consultation des offices que la révision de l'ordonnance était actuellement prématurée.

Dans le cadre de la consultation des offices, nous avons été invités à nous prononcer sur la révision de l'ordonnance sur la protection des données personnelles dans l'administration fédérale. Dans notre réponse, nous avons en particulier demandé que les bases légales requises pour l'ordonnance soient créées dans le cadre de la révision de la loi sur le personnel de la Confédération. Nous avons en outre relevé que les dispositions importantes de l'ordonnance qui contiennent des règles de droit soient ancrées dans la loi. En ce qui concerne les autorisations d'accès, nous avons relevé que le cercle des personnes et services devant avoir accès à l'ensemble des données dans le système administratif des données personnelles BV-PLUS était trop large. Nous avons donc demandé que les réglementations concernant les autorisations d'accès soient plus restrictives. Nous avons également requis que l'ordonnance règle dans quel but les personnes autorisées devaient avoir un droit d'accès à l'ensemble des données dans BV-PLUS.

Suite à une séance avec l'Office fédéral du personnel (OFPER), chargé de la coordination, ainsi qu'avec l'Office fédéral de la justice, la Chancellerie de la Confédération et d'autres conseillers à la protection des données de l'administration fédérale, nous sommes parvenus, au terme de la consultation des offices, à la conclusion qu'il était prématuré de procéder à une révision de l'ordonnance. Le concept d'automatisation du traitement des dossiers du personnel se trouve encore dans une phase peu avancée. Il convient d'empêcher qu'une ordonnance provisoire créée une situation de fait accompli, dont la nécessité n'a pas encore fait l'objet d'examens approfondis. Il en va de même de l'introduction des évaluations et des conventions d'objectifs dans BV PLUS. Nous avons encore relevé que la seule révision actuellement nécessaire de l'ordonnance concernait la réglementation des activités accessoires. Toutefois, cette

lacune du droit peut être momentanément tolérée dans la mesure où les travaux de révision de la loi sur le personnel de la Confédération démarreront prochainement. L'OFPER a donc suspendu les travaux de révision de l'ordonnance jusqu'à ce que les bases nécessaires soient créées dans la loi sur le personnel de la Confédération.

1.6.5 Ordonnance concernant des mesures en matière de lutte contre le travail au noir

Dans le cadre de la consultation des offices, nous avons pris position sur le projet d'ordonnance d'exécution de la loi fédérale concernant des mesures en matière de lutte contre le travail au noir. Nous avons relevé le degré de précision insuffisant des normes concernant la protection des données, surtout celles concernant l'échange d'informations entre autorités et leurs droits d'accès.

Les données concernant le travail au noir sont sensibles. Les normes régissant le traitement de ces données doivent présenter un haut degré de précision qui, à notre avis, n'est pas donné dans l'ordonnance d'exécution de la loi fédérale concernant les mesures en matière de lutte contre le travail au noir. Nous avons donc, dans le cadre de la consultation des offices, critiqué le degré de précision des normes de cette ordonnance. Or, tout traitement de données sensibles nécessite une base légale claire et précise. Nous avons à ce sujet précisé qu'une base légale au sens matériel devait contenir des dispositions concrètes concernant les données personnelles traitées, les droits d'accès et leur étendue, ainsi que leur communication.

Nous avons en particulier critiqué le fait que le texte de l'ordonnance ne décrit pas concrètement l'information mutuelle des autorités participantes. La formulation proposée laisse au bon vouloir des autorités participantes le soin de décider qui communique quelles données, à qui, quand et dans quel but. Nous avons demandé au Secrétariat d'Etat à l'économie (SECO), chargé de la coordination, de réglementer dans le texte de l'ordonnance l'échange d'informations entre autorités.

Nous avons également critiqué la réglementation du droit d'accès des autorités participantes. Selon le texte de l'ordonnance, toute autorité participante peut intervenir, grâce à un droit d'accès étendu, dans les traitements de données des autres autorités. Plusieurs autorités portent donc dans la même mesure la responsabilité pour un seul et même traitement de données. Dans ces circonstances, nous avons requis que l'ordonnance indique clairement quelle autorité à accès à quelles données, et quel est l'étendue de cet accès. Le cas échéant, il convient de prévoir une matrice d'accès.

Lors d'une séance, le SECO a accepté nos objections et s'est engagé à remanier l'ordonnance dans le sens de celles-ci. Toutefois, nous avons dû ultérieurement constater que le nouveau projet d'ordonnance ne tenait que partiellement compte des objections que nous avions alors formulées et que nous ne figurions pas sur la liste de la seconde consultation des offices.

1.7 Economie et commerce

1.7.1 Le droit d'accès et de rectification dans le domaine du renseignement commercial et des informations sur les crédits

Comme nous l'avons mentionné dans notre dernier rapport d'activités, nous avons vérifié en 2005 auprès de quatre grandes entreprises de renseignement commercial comment celles-ci garantissaient les droits des personnes concernées en matière de protection des données. Bien que nos appréciations aient en général été positives, cela ne signifie pas que les personnes concernées ne rencontrent pas de problèmes.

Nous avons contrôlé comment les diverses sociétés de renseignement commercial réagissaient aux demandes d'accès, de rectification et de destruction des données. Les sources d'information sur lesquelles nous nous sommes basés ont été d'une part la documentation que nous avions demandée, d'autre part une visite sur place, divers entretiens et des correspondances. Selon les faits que nous avons constatés, on peut admettre que les dispositions légales ont été respectées, aussi bien en ce qui concerne le contrôle d'identité que les délais et les frais. Cela signifie que les entreprises contrôlées vérifient l'identité de la personne requérante avant de fournir un renseignement en vertu de la loi sur la protection des données et qu'elles fournissent les renseignements gratuitement et dans un délai maximal de 30 jours, sauf dans les cas d'exception prévus par la loi. Les exigences de la protection des données sont également respectées au niveau matériel puisque nous avons pu observer que les renseignements fournis étaient complets et compréhensibles. En ce qui concerne les demandes de rectification et de destruction des données, nous n'avons pas non plus fait de constatations permettant de conclure que les exigences légales ne seraient pas respectées. Malgré cette appréciation positive de la situation, nous continuons à être sollicités par des personnes concernées rencontrant des problèmes avec des entreprises de ce secteur. Nous ne pouvons qu'émettre des suppositions sur les raisons possibles de ces difficultés. Nous partons du principe que les demandes que nous recevons peuvent être classées en deux catégories. La première comprend tous les

cas dans lesquels des problèmes sont apparus au niveau de la comparaison automatique des données (matching); en d'autres termes, il s'agit de cas dans lesquels deux personnes ont été confondues, par exemple deux personnes ayant des noms presque identiques et habitant la même rue. La deuxième catégorie comprend les demandes de rectification et de destruction des données, où le fait qui a mené à l'enregistrement des données n'a pas pu être clairement établi. Ces cas reflètent un conflit manifeste entre les intérêts des entreprises de renseignement et leurs clients d'une part et les personnes concernées d'autre part.

1.8 Finances

1.8.1 La protection des données dans le trafic international des paiements (SWIFT)

La majeure partie du trafic international des paiements est effectuée par l'intermédiaire de la Society for Worldwide Interbank Financial Telecommunication (SWIFT), sise en Belgique. En juin 2006, une information a été rendue publique par les médias: les autorités américaines de lutte contre le terrorisme auraient accès aux données des transactions bancaires du réseau mondial de la SWIFT. Sur la base des informations reçues, nous avons procédé à des éclaircissements avec les principaux responsables du secteur bancaire en Suisse et agi à différents niveaux en vue de trouver une solution à cette affaire SWIFT.

La société SWIFT, dont le siège est en Belgique, est la plus grande entreprise mondiale spécialisée dans le trafic international des paiements. Elle dispose de deux archives dans lesquelles elle conserve la totalité des données des transactions durant 124 jours. La presse américaine a révélé que l'administration gouvernementale avait désormais accès à des données relatives aux transactions financières, par l'intermédiaire des archives de SWIFT conservées aux Etats-Unis et avec l'aide de SWIFT. On ne dispose jusqu'ici d'aucune autre information précise.

La protection des données est indubitablement l'un des aspects majeurs du volet juridique de l'affaire SWIFT. Pour cette raison, les autorités de protection des données de nombreux pays ont entrepris des investigations. SWIFT étant domiciliée en Belgique, l'enquête menée par la Commission belge de la protection de la vie privée revêt une haute importance. Cette commission a constaté dans son rapport que la SWIFT avait commis plusieurs infractions aux droits belge et européen de la protection des données.

Sur la base du rapport de la commission belge et de nos propres recherches, nous avons constaté que SWIFT ne traitait pas de données personnelles en Suisse. Il restait encore à répondre à la question de la responsabilité en matière de protection des données des prestataires de services financiers sis dans notre pays. Le rapport du PFPDT sur cette question se trouve à l'annexe 4.1.

En résumé, il convient d'attirer l'attention sur deux points problématiques: d'une part, même après avoir été mis au courant de l'affaire SWIFT, les prestataires financiers n'ont pas informé leurs clients des risques d'accès à leurs données en cas de virement international (manque de transparence du traitement des données); d'autre part, la consultation de données contenues dans les transactions par l'administration américaine pose le problème du transfert de données dans un pays ne possédant pas une réglementation en matière de protection des données de portée équivalente.

La clarification des questions de protection des données autour de l'affaire SWIFT a eu lieu en collaboration avec de nombreuses autorités étrangères de protection des données, notamment avec le Groupe de travail «article 29» de l'Union européenne; dans ce cadre aussi, nous continuerons à nous engager en faveur d'une solution conforme au droit de la protection des données. Enfin, dans cette affaire, nous avons également informé la Commission de gestion du Conseil national (Sous-commission DFF/DFE) qui a pris le problème en main.

Au niveau suisse, l'affaire SWIFT demande encore que des mesures soient prises en matière de protection des données. Il faut négocier au niveau politique une solution qui tienne compte des nécessités de la lutte contre le terrorisme, tout en respectant les règlements en matière de protection des données de tous les pays, donc aussi la loi suisse sur la protection des données. Par ailleurs, dans la mesure où ils le peuvent, ce sont les prestataires financiers suisses qui doivent agir en premier lieu car ils doivent notamment garantir la transparence et informer des risques d'accès en cas de paiements internationaux.

1.9 International

1.9.1 Conférence internationale des commissaires à la protection des données

La 28ème Conférence internationale des commissaires à la protection des données et à la vie privée s'est déroulée à Londres les 2 et 3 novembre 2006. Sous le thème «Vers une société de surveillance?», les dangers de la société de surveillance étaient au centre des débats. Les commissaires ont fait le constat que la société de surveillance était aujourd'hui une réalité et ont souligné l'importance que revêt dans ce contexte le droit à la protection des données. Celui-ci constitue un droit fondamental nécessaire à l'exercice des autres droits et des libertés fondamentales dans une société démocratique. Les commissaires ont en outre adopté une résolution sur la protection de la vie privée et les moteurs de recherche. Ils ont unanimement soutenu une initiative de la CNIL visant à améliorer la communication sur la protection des données et de rendre cette dernière plus effective.

A l'invitation du Commissaire britannique à la protection des données et à l'information, 58 autorités de protection des données provenant du monde entier et des représentants d'organisations internationales, de l'économie et de la science se sont réunis à Londres pour débattre de la société de surveillance, à l'occasion de la 28ème Conférence internationale des commissaires à la protection des données. La Suisse y était représentée par le Préposé fédéral à la protection des données et à la transparence, ainsi que par les préposés des cantons de Bâle-Campagne, Zoug et Zurich.

La partie centrale de la conférence était consacrée aux implications de la société de surveillance. Le Commissaire britannique à la protection des données et à l'information avait mandaté une vaste étude sur le phénomène de la société de surveillance en vue de lancer un débat public sur les développements préoccupants auxquels les sociétés démocratiques sont actuellement confrontées (l'étude est disponible sur le site de la conférence www.privacyconference2006.co.uk). La société de surveillance est devenue une réalité et les dérapages sont inévitables si des limites ne sont pas posées.

Les traitements de données opérés dans le cadre de la société de surveillance ont une influence grandissante dans nos vies respectives, sur nos comportements et sur nos styles de vie. Ils engendrent des risques pour la protection des données et le respect des droits et libertés fondamentales, et notamment la vie privée. Certaines activités de surveillance sont cependant nécessaires, par exemple pour lutter contre le terro-

risme et la grande criminalité ou améliorer les soins de santé. Elles peuvent avoir des effets bénéfiques pour l'individu et pour la société. Toutefois, il convient d'examiner ce qui est acceptable du point de vue d'un Etat démocratique respectueux des droits et des libertés fondamentales et de fixer les limites à la surveillance. La surveillance incontrôlée a des effets négatifs non seulement du point de vue du droit à la protection des données et à la vie privée, mais peut aussi mettre en péril d'autres valeurs d'un Etat de droit. L'excès de surveillance peut notamment contribuer à créer et à entretenir un climat de suspicion, saper la confiance des citoyens et citoyennes dans les institutions en place et avoir un impact sur la nature même de la société. Il existe en outre un risque croissant de discrimination et d'exclusion sociale. Sans contester la nécessité de certaines mesures, les commissaires ont ainsi souligné l'importance du droit à la protection des données et à la vie privée comme droit de l'homme. Les réglementations de protection des données et de la vie privée permettent d'imposer des restrictions légitimes à la surveillance. Elles sont cependant insuffisantes si elles ne sont pas accompagnées de mesures permettant de garantir le respect des principes de protection des données, et notamment le principe de transparence. Des évaluations systématiques des impacts sur la vie privée des techniques de surveillance envisagées ou mises en place devraient également être effectuées. Les réglementations doivent aussi être évaluées pour voir si elles apportent une réponse adéquate au défi actuel. La société de surveillance doit faire l'objet de vastes débats publics. Tous les acteurs concernés doivent collaborer pour enrayer les conséquences négatives de ces développements sécuritaires. Ils doivent œuvrer à gagner et à renforcer la confiance du public. Les citoyens doivent être convaincus que chaque intrusion dans leur vie privée est nécessaire et proportionnée. Les abus doivent pouvoir être dénoncés et des sanctions (notamment pénales) prononcées lorsqu'il y a atteinte à la vie privée. Dans ce contexte, les autorités de protection des données ont un rôle essentiel à jouer pour contrôler et repousser la surveillance excessive. Les commissaires à la protection des données ont ainsi apporté leur soutien à une initiative de la Commission nationale de l'informatique et des libertés (CNIL) en vue de réaffirmer l'importance fondamentale de la protection des données et de la vie privée dans un monde en mutation constante. La déclaration «communiquer dans le domaine de la protection des données et rendre cette communication plus efficace» (voir annexe 4.4) est un manifeste visant à accroître l'effectivité de la protection des données. Comme le relevait le président de la CNIL, M. A. Türk, face aux risques liés aux exigences de la sécurité collective et aux développements technologiques (biométrie, géolocalisation, vidéosurveillance, Internet, RFID, etc.), «les autorités de protection des données doivent provoquer une prise de conscience collective et se rassembler pour lancer des initiatives coordonnées, reposant principalement sur une nouvelle stratégie de communication, un accroissement des capacités d'expertise, une évaluation et un renforcement de leurs moyens

d'action, et un soutien aux travaux menant à la reconnaissance d'un droit universel à la protection des données. Le capital de notre identité et de notre vie privée est chaque jour menacé. Il y a urgence à le préserver. Comme le capital environnemental de l'humanité, il risque, lui aussi, d'être si gravement atteint qu'il ne puisse être renouvelé.» Une attention particulière devra être apportée à la sensibilisation du public.

Les commissaires ont en outre adopté deux résolutions. L'une concerne le respect de la vie privée et les moteurs de recherche (voir annexe 4.6). Elle appelle en particulier les fournisseurs de moteurs de recherche à respecter les exigences de la protection des données et notamment à informer les utilisateurs de manière transparente des traitements de données réalisés lors de l'utilisation de leurs services et à limiter le nombre de données personnelles collectées (principe de minimisation des données). La seconde résolution concerne les modalités pratiques d'organisation de la conférence (voir annexe 4.5). Les commissaires ont également procédé à l'accréditation des autorités de protection des données d'Andorre, du Liechtenstein, d'Estonie, des provinces canadiennes du Nouveau-Brunswick, des Territoires du Nord-Ouest et du Nunavut, ainsi que de Gibraltar. Enfin, ils ont dressé un premier bilan positif du suivi de la déclaration de Montreux (voir notre 13ème rapport d'activités 2005/2006, ch. 9.2.1 et annexe 11.2). En particulier l'appel des commissaires à l'élaboration d'un instrument juridique a reçu un écho positif, notamment auprès de la commission onusienne du droit international qui l'a inscrit à son programme de travail. De même, le secrétariat général du Conseil de l'Europe s'est engagé à appuyer les démarches en vue de l'adhésion d'Etats non membres du Conseil de l'Europe à la Convention 108. Enfin, la nécessité de renforcer le caractère universel du droit à la protection des données ressort des documents du Sommet de la société de l'information de Tunis (16-18 novembre 2005, http://www.itu.int/wsis/documents/doc_multi.asp?lang=fr&id=2331|2304) et de la déclaration du Sommet des chefs d'Etats et de gouvernement de la francophonie de Bucarest (28-29 septembre 2006, http://www.francophonie.org/doc/txt-reference/decl-bucarest-2006.pdf).

1.9.2 Conférence européenne des commissaires à la protection des données

La Conférence européenne des commissaires à la protection des données s'est tenue à Budapest du 24 au 25 avril 2006. Les commissaires européens ont adopté à l'unanimité une déclaration relative à l'introduction du principe de disponibilité des données dans le cadre du renforcement de la coopération policière et judiciaire au sein de l'Union européenne.

A l'invitation du Commissaire à la protection des données et à l'information de la Hongrie, les commissaires européens à la protection des données ont tenu leur conférence de printemps du 24 au 25 avril 2006 à Budapest. Les commissaires de 34 Etats européens, le contrôleur européen à la protection des données et les représentants des autorités de contrôle communes Europol et Schengen ont pris part à la conférence. La Suisse était représentée par le Préposé fédéral à la protection des données et les préposés à la protection des données des cantons de Bâle-Campagne, Zoug et Zurich.

Lors de son message de bienvenue, le président de la République de Hongrie, Mr. László Sólyom, a rappelé l'importance du droit à la protection des données dans le monde actuel et a en particulier souligné le fait que la lutte contre le terrorisme ne doit pas se faire au détriment du droit à l'autodétermination informationnelle. La conférence a ainsi permis aux commissaires de faire le point sur différents dossiers d'actualité, notamment le traitement de données personnelles dans le domaine de la coopération policière et judiciaire, les défis des nouvelles technologies invasives, les systèmes d'alerte professionnelle dans les entreprises, le développement du dossier électronique du patient, le traitement des données génétiques, la recherche scientifique à des fins historiques.

Les commissaires se sont également penchés sur l'efficience de leurs actions. Partant du constat qu'actuellement la plupart des autorités nationales de protection des données n'ont pas les ressources suffisantes pour accomplir leurs tâches, les commissaires européens se sont accordés sur la nécessité de fixer des priorités, de privilégier la concertation et de collaborer avec d'autres acteurs de la société civile (organisations de protection des consommateurs, organisations de défense des libertés individuelles, etc.). Ils ont également relevé l'importance de la visibilité de leurs actions et des objectifs poursuivis. De même, il est important que l'accomplissement de leurs tâches soit soumis à évaluation. Les autorités ne sont pas en mesure de traiter toutes les demandes qui leur parviennent et d'intervenir pour chaque plainte déposée. Il est

souhaitable de fixer des critères d'intervention et de mettre la priorité pour les cas où les personnes concernées se trouvent dans un rapport de faiblesse par rapport au responsable de traitement, où le traitement de données personnelles est un enjeu important et où le droit à l'autodétermination informationnelle pourrait être limité de manière injustifiée. L'autorité britannique de protection des données prend ainsi en considération notamment les critères suivants pour déterminer l'opportunité d'agir: risque sérieux pour l'individu, nombre de personnes concernées, nécessité de clarifier des dispositions légales ou des principes de protection des données, risque de répétition ou de persistance de l'atteinte, nécessité de faire un «exemple», rapport entre le coût de mise en conformité à la loi pour l'organisation impliquée et l'effet attendu, caractère délibéré de l'atteinte.

La Conférence a accrédité 3 nouveaux Etats: l'Ex-République yougoslave de Macédoine, la Roumanie et la Slovénie. Andorre a quant à lui obtenu le statut d'observateur. Les commissaires ont finalement adopté à l'unanimité une déclaration concernant la coopération policière et judiciaire, en particulier le projet de décision-cadre de l'Union européenne relative au principe de disponibilité. La Conférence rappelle en particulier que l'échange d'informations personnelles entre les autorités de poursuite ne peut intervenir que dans le respect de règles de protection des données. Aux yeux des commissaires européens, il est indispensable que l'ensemble du domaine de la coopération policière et judiciaire soit régi par des règles harmonisées assurant un haut niveau de protection des données. En marge de la 28ème Conférence internationale des commissaires à la protection des données (voir ci-dessus ch. 1.9.1), la Conférence européenne a adopté une deuxième déclaration concernant le projet de décision cadre de l'Union européenne régissant la protection des données dans le domaine de la coopération policière et judicaire (voir notre 13ème rapport d'activités 2005/2006, ch. 9.1.2). Dans cette déclaration, les commissaires rappellent que l'introduction du principe de disponibilité est liée à l'adoption d'un cadre adéquat de protection des données pour l'ensemble des traitements effectués à des fins de coopération policière et judiciaire. Ce cadre doit garantir un haut niveau de protection des données qui soit cohérent avec les dispositions de la directive européenne 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. En particulier, il ne doit pas y avoir de distinction entre le fait que les données proviennent d'un traitement indigène ou qu'elles aient été reçues d'une autorité étrangère.

1.9.3 Case Handling Workshop - Groupe de travail européen sur le traitement de cas relevant de la protection des données

Le groupe de travail «Case Handling Workshop», mis en place par la Conférence européenne des Commissaires à la protection des données, a pour objectif d'examiner et de concrétiser les moyens de collaboration et de coopération entre autorités de contrôle de protection des données. Lors de ses dernières réunions, le groupe de travail a orienté ses travaux sur les méthodes de traitement de cas concrets similaires rencontrés par différentes autorités nationales.

Sur la base du mandat attribué par la Conférence européenne des Commissaires à la protection des données, le groupe de travail européen sur le traitement de cas relevant de la protection des données («Case Handling Workshop») a, lors de ses deux réunions en 2006 à Madrid et Athènes, mis en application la nouvelle orientation décidée l'année précédente.

En effet, lors de ses premières réunions, le groupe de travail - alors dénommé «Complaints Handling Workshop» (groupe de travail sur le traitement des plaintes) - s'était concentré sur les méthodes de contrôle utilisées par les autorités de protection des données en fonction de leurs compétences légales respectives. Ces échanges d'information sur les contrôles effectués dans les différents Etats ont permis une meilleure connaissance des rôles, des pouvoirs de sanction, des instruments et des compétences des autres autorités de contrôle nationales.

Au cours de ses activités, le groupe de travail s'est toutefois vu confronté à un double problème: L'accroissement du nombre de participants d'une part, la difficulté de concrétiser les échanges d'informations d'autre part. Approchant la soixantaine de participants, le groupe de travail a procédé à un examen de son mode de fonctionnement. Tout en souhaitant conserver un caractère informel favorisant les échanges d'expériences, le groupe a ainsi décidé d'organiser de manière plus efficiente les différentes interventions des participants, de mieux coordonner le choix des thèmes des réunions (notamment avec les travaux en cours du Groupe de travail «article 29» de l'Union européenne) et de concentrer ses travaux sur des cas concrets. Le groupe a ainsi été renommé «Case Handling Workshop» (Groupe de travail européen sur le traitement de cas relevant de la protection des données).

Ces modifications ayant été avalisées par la Conférence européenne des Commissaires à la protection des données qui s'est tenue au printemps 2005 à Cracovie, le Groupe de travail a orienté les travaux de ses deux réunions de 2006 sur des cas concrets. Ainsi la réunion de mars 2006 à Madrid s'est focalisée sur les manières de traiter les cas de protection des données relevant du secteur public. Nous avons à cette occasion présenté les problèmes rencontrés lors des différentes étapes du contrôle que nous avons effectué auprès de l'Office fédéral de la police afin de vérifier l'information ultérieure des personnes concernées (cf. nos 12ème rapport d'activités 2004/2005, chiffre 3.1.1 et 13ème rapport d'activités 2005/2006, chiffre 3.1.4). La présentation de ce cas d'espèce a permis de constater de nombreuses similitudes avec des contrôles menés par d'autres autorités nationales dans le secteur public (difficultés dans l'établissement des faits et dans la recherche de solutions d'amélioration, refus des recommandations, utilisation des voies de recours). La réunion de novembre 2006 à Athènes a quant à elle été consacrée au traitement de cas concrets relevant du gouvernement électronique d'une part et de la vidéosurveillance d'autre part. Ce dernier thème a permis un échange fructueux sur les nombreux problèmes (bases légales, proportionnalité, accès aux données, rôles des différents acteurs, réutilisation des données, effacement des données, etc.) constatés lors de la mise en place de caméras de vidéosurveillance dans le cadre de grandes manifestations sportives telles que les Jeux olympiques d'Athènes en été 2004 ou le Championnat d'Europe de football (EURO 08) qui se déroulera en Suisse et en Autriche en 2008.

Le groupe de travail, dont la prochaine réunion en 2007 se déroulera à Helsinki, va poursuivre ses activités en ayant pour objectif d'améliorer la collaboration entre autorités nationales de contrôle. Pour ce faire, il procédera à une comparaison des méthodes de traitement de cas concrets similaires et des solutions qui y sont apportées, que ce soit dans le cadre de plaintes, d'inspections, d'analyses ou de contrôles d'office.

1.9.4 Groupe de travail international «Protection des données dans le domaine des télécommunications»

Lors de sa 40ème séance à Berlin, le groupe de travail international «Protection des données dans le domaine des télécommunications» a discuté, entre autres, des thèmes de l'informatique de confiance (Trusted Computing), de la gestion numérique des droits (Digital Rights Management) ainsi que de la téléphonie par Internet (VoIP).

En septembre 2006, le groupe de travail international «Protection des données dans le domaine des télécommunications» (International Working Group on Data Protection in Telecommunications) a tenu sa 40ème séance à Berlin, à laquelle nous avons pris part. Le groupe a traité entre autres des sujets suivants:

Trusted Computing (TC) /Digital Rights Management (DRM): Dans un document de travail(http://www.datenschutz-berlin.de/doc/int/iwgdpt/WP_Trusted_Computing_en.pdf), le groupe recommande que les gouvernements tiennent compte des risques liés à la protection des données qui peuvent se présenter lors de la mise en œuvre de ces technologies. Il appelle les gouvernements à créer des réglementations permettant de lutter contre les atteintes à la sphère privée causées par TC/DRM. Le groupe recommande en outre aux développeurs de logiciels et aux fournisseurs de produits TC/DRM de prendre les mesures de protection des données qui sont dans leur domaine d'influence.

Un autre document sur le thème de la téléphonie par Internet (Voice-over-IP, VoIP) a été adopté et publié (http://www.datenschutz-berlin.de/doc/int/iwgdpt/WP_VoIP_en.pdf): l'utilisation de la téléphonie par Internet a connu un énorme essor ces derniers temps. Pour éviter que la sécurité et la sphère privée n'en souffrent, il est nécessaire d'élaborer des réglementations qui garantissent que la téléphonie par Internet respecte au moins les mêmes exigences de protection des données et de sécurité que celles qui doivent être appliquées pour la téléphonie usuelle par lignes terrestres et ondes radio (téléphonie mobile). Les fournisseurs de prestations de téléphonie par Internet doivent notamment rendre leurs clients attentifs aux risques ainsi qu'aux moyens de les contrer, ils doivent proposer un cryptage inter-opérateurs de bout-en-bout et traiter uniquement les données qui sont nécessaires à la fourniture de la prestation ou qui sont exigées par des lois.

Tous les documents publiés peuvent être consultés sur le site www.iwgdpt.org.

2 Principe de la transparence

2.1 Loi fédérale sur le principe de la transparence dans l'administration

Le principe de transparence a été introduit dans l'administration fédérale le 1er juillet 2006. Il crée un droit d'accès aux documents officiels, directement invocable en justice. Il attribue en outre de nouvelles tâches au Préposé fédéral à la protection des données: désormais, celui-ci est l'organe de conseil et de médiation en matière de transparence et se dénomme Préposé fédéral à la protection des données et à la transparence (PFPDT).

La loi fédérale sur le principe de la transparence dans l'administration, abrégée loi sur la transparence (LTrans), est entrée en vigueur le 1er juillet 2006. Elle rend effectif le passage du principe du secret de l'administration au principe de la transparence. Ainsi, il est désormais possible d'accéder aux documents officiels élaborés depuis l'entrée en vigueur de la loi, le 1er juillet 2006. Ces documents peuvent être consultés sur place ou obtenus en copie. Il n'est pas nécessaire de justifier d'un intérêt particulier lors d'une demande d'accès adressée à l'autorité compétente ; en outre, la demande n'est soumise à aucune forme. Si l'accès est refusé, le requérant peut adresser au PFPDT une requête en médiation. En tant que médiateur, le PFPDT recherche un accord rapide entre l'autorité concernée et le requérant. La procédure se déroule par écrit ou oralement. En cas d'échec de la médiation, le préposé peut adresser une recommandation et le requérant a encore la possibilité d'agir en justice.

Outre cette fonction d'organe de médiation, le préposé a également une fonction de conseiller: il est un centre de compétence pour les autorités et les particuliers pour toute question en rapport avec le principe de la transparence et l'accès aux documents officiels.

Conformément à la loi sur la transparence, le préposé doit évaluer l'application, l'efficacité et en particulier les coûts engendrés par la mise en œuvre de la présente loi. Il en fait rapport au Conseil fédéral, pour la première fois trois ans à compter de l'entrée en vigueur de la loi (soit le 1er juillet 2009). Au cours des sept premiers mois qui ont suivi l'entrée en vigueur de la loi sur la transparence, nous avons reçu six demandes de médiation. Nous allons brièvement commenter ci-après les trois procédures aujourd'hui closes.

2.2 Procédure de médiation dans le cadre du principe de la transparence

2.2.1 Recommandation au Tribunal pénal fédéral: «Rapport sur les griefs relatifs au faible nombre d'actes d'accusation prononcés par le Ministère public de la Confédération»

La loi sur la transparence accorde au Préposé fédéral à la protection des données et à la transparence de larges compétences lorsqu'il s'agit d'obtenir des renseignements et de consulter des documents dans le cadre d'une procédure de médiation. Le Tribunal pénal fédéral a toutefois refusé de nous garantir la consultation d'un rapport. La question de savoir si le rapport tombait sous le coup de la loi sur la transparence et était de ce fait accessible a dû être laissée ouverte.

Une personne a demandé d'accéder au rapport élaboré par le Tribunal pénal fédéral sur les griefs concernant le faible nombre de mises en accusation prononcées par le Ministère public de la Confédération. Suite à sa demande d'accès transmise oralement, il lui a été répondu qu'aucune autre information ne serait donnée qui irait plus loin que le communiqué de presse publié à ce propos. Suite à une autre demande, cette fois écrite, il lui a été communiqué qu'elle recevrait une réponse en temps voulu. Au terme du délai de 20 jours - prévu par la loi sur la transparence - pour prendre position, la requérante, n'ayant pas obtenu de réponse, nous a transmis une demande en médiation.

Nous avons enjoint le Tribunal pénal fédéral de nous remettre le rapport en question afin d'apprécier la situation. Le Tribunal s'y est refusé et nous a communiqué, entre autres, que le rapport n'était pas un document à caractère administratif et ne tombait donc pas dans le domaine d'application de la loi sur la transparence. A ses yeux, nous n'étions pas compétents en la matière.

En ce qui concerne la question de la compétence, nous avons entre autres précisé dans notre recommandation que dans les cas où il n'apparaît pas d'emblée que le principe de la transparence est inapplicable, nous examinons toute demande en médiation remise dans les formes et les délais prévus. Cette position repose sur la conception même de la loi sur la transparence: celle-ci prévoit que la procédure en médiation doit obligatoirement être menée avant qu'une personne à qui l'accès a été refusé obtienne de l'autorité compétente une décision et qu'elle puisse ensuite

attaquer celle-ci en justice. Si nous n'entrions pas en matière sur une demande en médiation dans des cas où l'applicabilité de la loi sur la transparence est contesté, nous refuserions au requérant l'exercice des droits qui lui reviennent d'après la loi sur la transparence et partant, le droit d'être entendu prévu par la Constitution fédérale (art. 29 al. 2 Cst.).

Nous n'avons pas pu apprécier de manière exhaustive la question de savoir si le rapport en question tombait sous le coup de la loi sur la transparence car le Tribunal pénal fédéral a refusé de nous en remettre un exemplaire. Cette attitude contrevient clairement à la loi sur la transparence car celle-ci octroie au préposé de larges droits quant à l'obtention de renseignements et à la consultation de documents en procédure de médiation. Le commentaire concernant l'ordonnance sur le principe de la transparence dans l'administration précise à cet égard ce qui suit: «L'autorité a donc l'obligation de fournir au préposé tous les documents dont il a besoin; elle ne peut se soustraire à ce devoir en invoquant la confidentialité ou le caractère secret des informations.» Il va de soi que le préposé et son secrétariat sont soumis au secret de fonction dans la même mesure que les autorités dont ils consultent les documents officiels ou dont ils obtiennent des renseignements (art. 20 LTrans).

En adoptant la loi sur la transparence, le législateur a clairement exprimé sa volonté que les citoyens aient accès aux documents officiels. Il a conféré au préposé une fonction importante en tant qu'organe de liaison et de médiation doté des compétences requises. Il lui a ainsi octroyé un rôle fondamental dans la procédure d'accès aux documents officiels (FF 2003 1869). Le préposé ne peut pas assurer cette tâche s'il ne peut consulter lesdits documents, malgré des dispositions législatives claires lui accordant un droit d'obtenir des renseignements et de consulter des documents. Si les autorités fédérales et les tribunaux fédéraux, qui sont soumis au principe de la transparence, dénient au préposé son droit de consultation, la loi sur la transparence demeure lettre morte.

Nous avons recommandé au Tribunal pénal fédéral de réexaminer le droit d'accès au rapport en question, compte tenu de tous les aspects de la loi sur la transparence. Cette recommandation se trouve à l'annexe 4.7.

2.2.2 Recommandation adressée à l'Office fédéral des transports: «Rapports annuels des exploitants de téléphériques»

La loi sur la transparence ne s'applique qu'aux documents qui ont été établis après son entrée en vigueur. L'accès à des documents établis à une date antérieure ne doit pas être accordé.

Une personne a demandé à l'Office des transports (OFT) de pouvoir accéder aux communications des exploitants de téléphériques dont les installations étaient mises en danger par le recul du permafrost et devaient être rénovées. Elle désirait avoir accès à tous les documents établis entre 1991 et 2006. L'OFT a informé cette personne qu'il ne possédait pas de listes des installations en danger et qu'aucun document concernant «la rénovation de téléphériques suite au recul du permafrost» n'avait été élaboré après le 1er juillet 2006. Pour cette raison, l'OFT a informé le requérant qu'il ne pouvait donner suite à sa demande d'accès.

Cette personne a déposé chez nous une demande en médiation, mentionnant que l'OFT lui avait refusé l'accès aux documents officiels souhaités.

Dans notre recommandation, nous avons précisé que la loi sur la transparence ne s'applique qu'aux documents qui ont été établis ou reçus par une autorité après l'entrée en vigueur de cette loi, à savoir après le 1er juillet 2006. En outre, il convient de prendre en considération que la loi sur la transparence ne donne au requérant qu'un droit, directement invocable en justice, de consulter des documents officiels. Cette personne ne peut pas se fonder sur la loi sur la transparence pour demander qu'une autorité fédérale établisse pour elle seule une document qui n'existe pas.

Nous sommes parvenus à la conclusion que l'OFT ne devait pas accorder l'accès aux documents souhaités en conformité à l'art. 21 de la loi sur la transparence. La recommandation peut être consultée à l'annexe 4.8.

2.2.3 Recommandation adressée au Département fédéral des affaires étrangères: «Détection précoce des risques en matière de visas»

Nous considérons que la liste du Département fédéral des affaires étrangères (DFAE) concernant la détection précoce de risques en matière de visas est un document qui est en principe accessible au public. Le DFAE a suivi notre recommandation et a accordé l'accès au document.

Dans le cadre des mesures visant à lutter contre l'octroi abusif de visas dans les représentations suisses à l'étranger, le DFAE a notamment établi une liste permettant d'identifier les pays comportant des risques particuliers dans ce domaine. Cette liste devait servir à mieux cibler les mesures spéciales de protection à prendre. Le DFAE a répondu par la négative à une demande d'accès à cette liste, invoquant le fait qu'une publication de la liste pouvaient peser sur les relations entre la Suisse et certains Etats et restreindre la marge de manœuvre de la Suisse en matière de politique extérieure. Il invoquait à cet égard l'art. 7 de la loi sur la transparence. A la suite de cette réponse, la personne en question a déposé chez nous une demande en médiation.

La liste en question répertorie toutes les représentations suisses à l'étranger qui accordent des visas. Sur la base de sept critères, chaque représentation a été examinée sous l'angle des risques d'obtention abusive de visas. Nous avons constaté que la plupart de ces critères présentaient un lien avec la statistique sur les visas, déjà accessible au public, ou étaient en rapport avec l'octroi de visas. Un classement des représentations suisses, et non des différents Etats, a été établi sur la base de ces critères. Du fait que ni les critères ni leur classement ne contenaient de déclarations ou d'appréciations sur d'autres Etats, nous avons considéré que le refus de l'accès sous l'angle de ces critères contrevenait à la loi sur la transparence.

Seul un critère se fondait sur des estimations et des appréciations de la situation actuelle dans les Etats accueillant la représentation. Nous avons estimé que la possibilité d'avoir accès à ce critère pourrait conduire les pays concernés à y voir une appréciation officielle de la Suisse concernant la situation dans leur pays. Il existerait ainsi une probabilité considérable que les relations avec un ou plusieurs pays s'en trouvent chargées négativement et qu'elles puissent ensuite en souffrir si le DFAE permettait l'accès à cette liste. Sur ce point, le DFAE avait donc refusé l'accès aux documents à juste titre.

Nous avons précisé dans notre recommandation (voir annexe 4.9) que la liste devait, à l'exception de ce critère, être rendue accessible. Le DFAE s'est conformé à notre recommandation.

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

3.1 Nouveau site web du PFPDT

Le Conseil fédéral a décidé à la fin de l'année 2003 d'uniformiser l'identité visuelle de tous les offices fédéraux dans le but de mettre en exergue l'appartenance à l'administration fédérale, d'en améliorer la transparence, de renforcer la confiance en l'Etat et d'accroître la crédibilité et la fiabilité des prestations publiques de la Confédération. Nous avons donc également adapté notre identité visuelle aux nouvelles exigences.

Parallèlement à l'entrée en vigueur le 1er juillet 2006 de la loi sur la transparence (LTrans) et du changement de nom de notre office de PFPD à PFPDT, nous avons mis en ligne notre nouveau site web. Ce dernier est maintenant conforme aux exigences élaborées par le service spécialisé «CD Bund» dans le cadre de l'uniformisation de l'identité visuelle de l'administration fédérale. Nous avons bien sûr dû nous procurer une nouvelle adresse Internet qui corresponde à la nouvelle désignation de notre office et soit conforme aux directives de CD Bund. C'est ainsi que www.edsb.ch est devenu www.edoeb.admin.ch. Vous pouvez également utiliser l'adresse www.leprepose.ch.

Nous avons profité de l'occasion pour élargir et améliorer notre offre sur le web, tout en veillant à ne pas trop nous écarter de la structure du contenu de notre ancien site afin de ne pas désorienter les visiteurs. La structure formelle du site (navigation) est la même que des sites des autres offices fédéraux et devrait en plus garantir l'accessibilité pour tous.

Une autre nouveauté est le portail d'information de l'administration fédérale. Le site www.news.admin.ch donne accès aux communiqués et exposés de la Chancellerie fédérale, des départements et de leurs services, donc également du PFPDT. Les personnes intéressées au domaine de la protection des données peuvent utiliser le service d'abonnement du portail d'information pour être informé chaque fois que le PFPDT publie un communiqué aux médias ou une prise de position, fait une annonce ou publie une nouvelle édition de son newsletter datum.

En plus du site web, nous avons également adapté l'ensemble de notre correspondance à la nouvelle identité visuelle de la Confédération.

3.2 Documents relatifs au principe de la transparence sur le site du PFPDT

En juillet 2006, la loi fédérale sur le principe de la transparence dans l'administration (LTrans) est entrée en vigueur. La loi favorise la transparence dans l'administration fédérale et donne aux particuliers et aux entreprises des droits importants en matière d'accès aux documents officiels. Dans le cadre de cette loi, le PFPDT a reçu de nouvelles fonctions et étendu la documentation disponible sur son site.

Dans son message relatif à la loi sur la transparence, le Conseil fédéral décrivait le rôle du Préposé fédéral à la protection des données et à la transparence comme étant celui «d'un centre de compétence en matière d'accès aux documents». Le PFPDT a rassemblé une vaste documentation afin d'être en mesure de répondre à ses nouvelles fonctions et de pouvoir conseiller aussi bien les particuliers que les offices fédéraux et les départements.

Exception faite des bases légales comme la loi et l'ordonnance, ainsi que l'introduction générale à la LTrans (voir sous la rubrique «Thèmes»), nous proposons un feuillet thématique pour les personnes désirant déposer une demande d'accès ainsi que des lettres-types pour les demandes d'accès et de médiation. Des réponses circonstanciées sont fournies aux questions les plus souvent posées (rubrique FAQ). Elles permettent d'éclairer divers aspects de l'accès aux documents officiels et aident en outre à clarifier des questions touchant aux procédures d'accès et de médiation. Les organes fédéraux concernés trouveront aussi sur notre site les guides et les schémas de procédures de l'Office fédéral de la justice. Ils leur permettront de répondre plus aisément aux demandes d'accès.

Si une procédure de médiation ne permet pas de parvenir à un accord, le PFPDT établit une recommandation. Afin de respecter les principes de la transparence, cette recommandation est publiée sur notre site web après avoir été anonymisée.

3.3 Les publications du PFPDT – nouveaux titres

Nous avons, dans l'exercice écoulé, continué à élargir la gamme des informations proposées sur notre site web. Nous avons rédigé quelques explications concernant les systèmes d'accès électroniques aux domaines skiables (dans la rubrique Thèmes – Protection des données – Autres thèmes, cf. également l'annexe 4.3). Dans la rubrique 'Thèmes – Protection des données – Secteur du travail', nous avons exposé quels sont les droits qu'un employeur a en matière de gestion de preuves en cas d'infraction ou de soupçon d'infraction au Code pénal commise par un employé au moyen d'Internet ou du courrier électronique.

Vous trouverez également sur notre site les prises de position concernant la communication aux autorités américaines de données des transactions bancaires du réseau SWIFT (Thèmes – Protection des données – Finances, cf. annexe 4.1) ainsi que concernant l'utilisation du numéro d'assuré AVS par les cantons (Thèmes – Protection des données – Autres thèmes – Documents d'identité et registres).

D'autre part, nous avons publié deux éditions de la nouvelle newsletter *datum* dans l'exercice écoulé.

Sur notre site web, nous proposons une documentation très complète sur le principe de la transparence (cf. ch. 3.2).

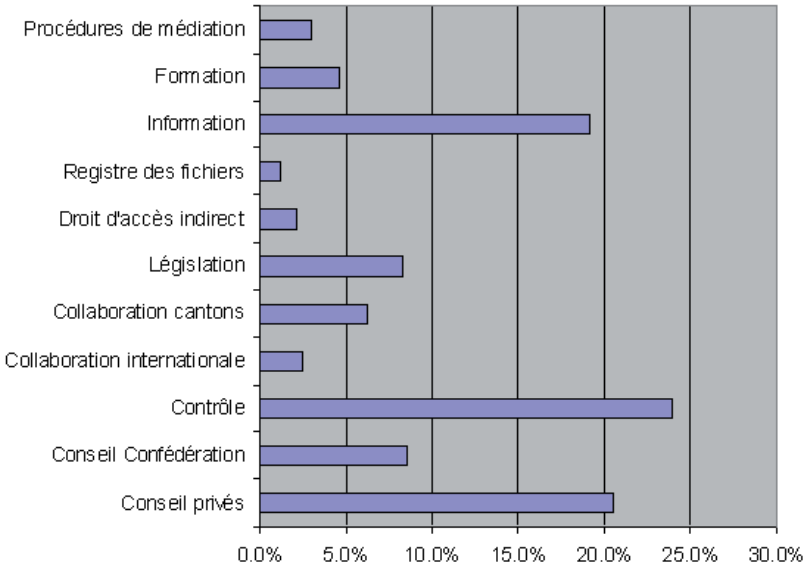
3.4 «Exagère-t-on en matière de protection des données?»

A l'occasion de la première Journée européenne de la protection des données, nous avons organisé en collaboration avec l'Europa Institut de l'Université de Zurich un colloque qui a eu lieu le 26 janvier 2007. Ce colloque avait pour titre «Exagère-t-on en matière de protection des données?» Hanspeter Thür a abordé avec trois invités un certain nombre de questions d'actualité touchant à la protection des données, et cela devant un public nombreux.

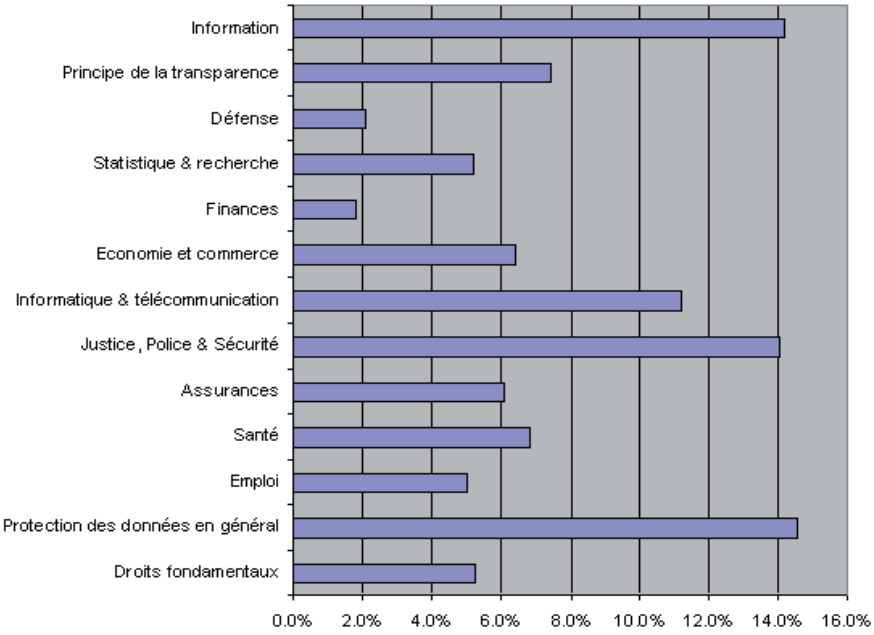
Casper Selg, directeur de l'émission d'informations «Echo der Zeit» de la radio suisse alémanique DRS, a dirigé cette table ronde qui, outre Hanspeter Thür, préposé fédéral à la protection des données et à la transparence (PFPDT), rassemblait trois invités: Anita Thanei, conseillère nationale PS/ZH, Filippo Leutenegger, conseiller national PRD/ZH, et Thomas Pletscher, membre de la direction d'economiesuisse. Un point a fait l'unanimité: le progrès technologique et la lutte contre le terrorisme constitueront de grandes défis pour la protection des données dans les années à venir. Alors que certains participants ont souligné que l'économie devrait collecter des données le plus librement possible tandis que des limites étroites devraient être imposées à l'Etat, Hanspeter Thür pour sa part a requis dans le domaine économique une plus grande transparence et plaidé en faveur d'une certification de la protection des données dans l'économie privée. En outre, le PFPDT a souligné les risques inhérents à la miniaturisation de la technique. L'Etat ne sera pas le seul à utiliser dorénavant des moyens toujours plus performants et meilleur marché; les mini-drones, les téléphones portables munis de caméras, les puces RFID et autres appareils permettront bientôt de surveiller tout un chacun.

3.5 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2006 au 31 mars 2007

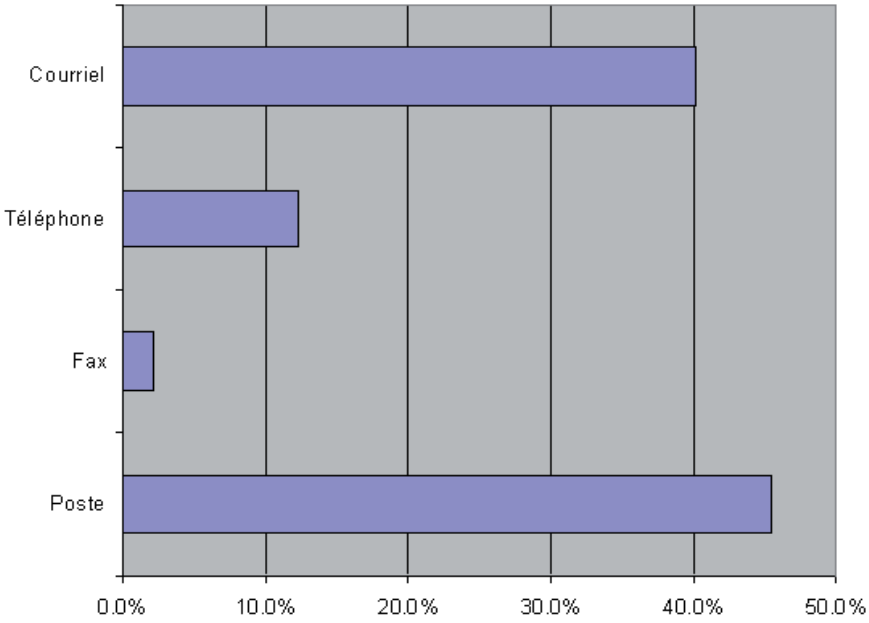
Charge de travail par tâches



Charge de travail par domaines



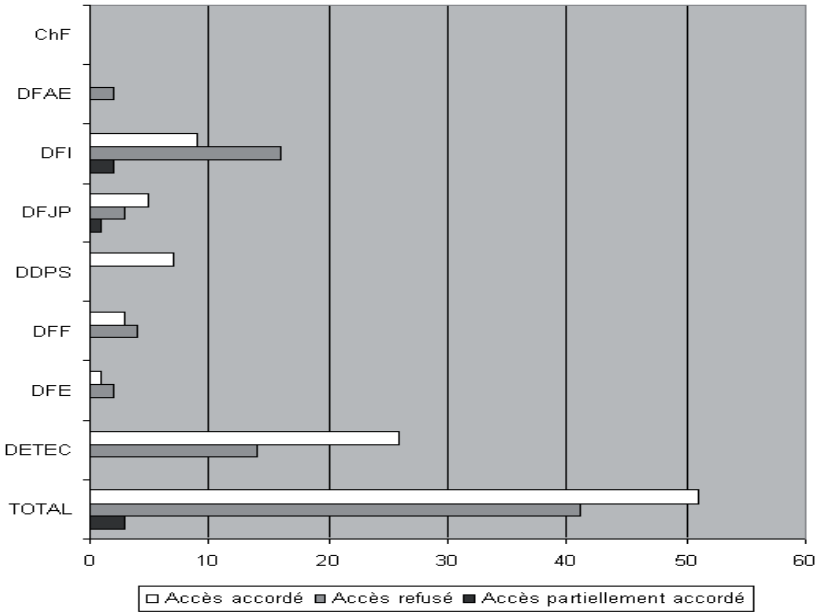
Provenance des demandes



3.6 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1er juillet 2006 au 31 décembre 2006)

Département	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement
ChF	0	0	0	0
DFAE	2	0	2	0
DFI	27	9	16	2
DFJP	9	5	3	1
DDPS	7	7	0	0
DFF	7	3	4	0
DFE	3	1	2	0
DETEC	40	26	14	0
TOTAL	95	51	41	3

Traitement des demandes d'accès



3.7 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 Conseil et Information: 8 personnes

Unité Surveillance: 11 personnes

Chancellerie: 3 personnes

4 Annexes

4.1 L'accès aux données des transactions bancaires du réseau mondial SWIFT – Avis du Préposé fédéral à la protection des données et à la transparence

I. Introduction

La plus grande partie du trafic international des paiements transite par la *Society for Worldwide Interbank Telecommunication* (SWIFT), qui a son siège en Belgique. Cela explique l'émoi suscité par les informations parues dans les médias depuis juin 2006, selon lesquelles l'administration des Etats-Unis peut accéder aux données des transactions SWIFT dans le cadre de sa lutte contre le terrorisme.

Sous l'angle juridique, l'un des aspects essentiels de cette affaire est incontestablement la protection des données. C'est pourquoi les autorités en charge de la protection des données ont, dans de nombreux pays, mené des investigations. SWIFT étant domiciliée en Belgique, l'étude de la *Commission de la protection de la vie privée* (CPVP) de ce pays revêt une importance particulière. La commission a publié les résultats de ses travaux le 27 septembre 2006.

Après avoir eu connaissance des faits par la presse, le Préposé fédéral à la protection des données et à la transparence (PFPDT) s'est renseigné auprès des acteurs principaux du secteur bancaire suisse. L'avis qu'il émet ci-après se fonde sur les informations ainsi recueillies, sur le rapport de la commission belge[1] et sur l'avis exprimé par le Conseil fédéral à l'intention de la Commission de gestion du Conseil national le 4 juillet 2006.

Dans son rapport, le Conseil fédéral ne s'est pas borné à présenter les faits les plus saillants: soucieux de légalité, il a également cherché à établir les compétences, car si une analyse en regard de la loi sur la protection des données relève du PFPDT, une éventuelle violation du secret dont bénéficient les clients des banques devrait être examinée par les tribunaux[2].

[1] *Avis n° 37 / 2006 du 27 septembre 2006 relatif à la transmission de données à caractère personnel par la SCRL SWIFT suite aux sommations de l'UST*, ci-après «*Rapport de la CPVP*», disponible dans sa version intégrale à l'adresse www.privacycommission.be.
[2] De l'avis du Conseil fédéral, sont en revanche incompétentes pour juger de la légalité des faits en question la Banque nationale suisse (BNS) et la Commission fédérale des banques (CFB).

D'un point de vue strictement juridique, le principe de territorialité limiterait également l'objet de l'étude. Selon nos informations, *SWIFT ne traite en Suisse aucune donnée personnelle*[3]. Dès lors, elle tombe sous le coup de la législation belge, et non suisse, sur la protection des données. La *CPVP* fait toutefois remarquer avec pertinence qu'en raison des relations entre les acteurs (SWIFT et prestataires de services financiers), il existe une responsabilité partagée quant au traitement des données[4].

Concrètement, la question à laquelle nous devons d'abord répondre en qualité d'autorité nationale est celle de la responsabilité, sous l'angle de la législation sur la protection des données, des prestataires de services financiers en Suisse. Pour ne pas perdre de vue le contexte global, il convient néanmoins d'examiner d'abord le comportement de SWIFT, et de ne pas limiter les conclusions à la situation en Suisse. L'affaire a en effet une dimension internationale, de sorte que des revendications qui ne se fondraient que sur la législation nationale en matière de protection des données ne suffiraient pas à résoudre le problème.

II. Responsabilité de SWIFT

A la suite des attentats de New York, SWIFT a été confrontée à des obligations imposées par diverses législations nationales (Belgique, Union européenne, Etats-Unis), finalement incompatibles. Comme le montre le rapport de la CPVP, SWIFT a décidé de donner largement suite aux exigences de la législation américaine. Bien qu'elle ait réussi lors de la négociation avec les autorités américaines – plus précisément avec le *US Department of the Treasury* – à se ménager des possibilités d'influence et de contrôle[5], les résultats que SWIFT a obtenus contreviennent sur plusieurs points aux législations belge et européenne sur la protection des données[6].

Compte tenu de la responsabilité conjointe de SWIFT et des prestataires de services financiers quant à la conformité du système de paiements aux exigences de la protection des données, l'ampleur des violations commises par SWIFT est essentielle pour l'analyse de la situation en Suisse.

[3] Ni la *SWIFT Switzerland GmbH*, ni la *SWIFT Switzerland National Member and User Group* ne sont chargés de tâches en relation avec le traitement de données concernant les transactions de la SWIFT belge.
[4] Cf. Rapport de la *CPVP,* p. 14 s.
[5] Cf. Rapport de la *CPVP*, p. 6 s.
[6] Cf. Rapport de la *CPVP*, pp. 16 ss.

Pour ce qui est du devoir d'information, le fait que plusieurs acteurs interagissent joue en effet un rôle. Si l'on fait abstraction du caractère légal ou non de l'accès aux données dont dispose l'administration américaine, le problème principal sous l'angle de la protection des données est celui du manque de transparence de la procédure pour les personnes concernées par le traitement des données. A cet égard, il convient de distinguer entre la responsabilité de SWIFT et celle des prestataires de services financiers.

En ce qui concerne l'obligation de traiter les données de manière transparente, les autorités belges parviennent à la conclusion que SWIFT aurait dû informer les prestataires de services financiers et les autorités de la protection des données de l'existence des sommations (subponeas) américaines vis-à-vis de SWIFT et des possibilités d'accès dont disposent les autorités des Etats-Unis[7].

Dans ce contexte, il convient de déterminer si les prestataires de services financiers ont failli à leur devoir d'information, en n'oubliant pas que dans le cadre du système de paiements SWIFT, ce sont exclusivement eux qui sont en contact avec les personnes concernées. Si l'on veut une transparence systématique, il est indispensable d'impliquer les prestataires de services financiers.

III. La responsabilité des prestataires de services financiers en Suisse

Pour tout paiement transitant par un institut financier, tant le commettant que le destinataire sont connus. En Suisse, lorsque des prestataires de services financiers interviennent dans la transaction, il y a nécessairement traitement de données personnelles au sens de la loi suisse sur la protection des données (art. 3, let. a et e, LPD). Dès lors, les prestataires de services financiers en question sont soumis à toutes les obligations que leur impose la législation sur la protection des données à l'égard des particuliers (LPD et OLPD).

Parmi les entorses possibles au droit, il convient de déterminer en premier lieu si le devoir d'informer a été respecté, ou plus précisément, si les prestataires de services financiers ont contrevenu aux principes de la bonne foi (art. 4, al. 2, LPD).

[7] Cf. Rapport de la *CPVP*, p. 23 s.

Comme nous avons déjà eu l'occasion de le souligner, la connaissance qu'ont les instituts financiers de la situation est décisive. Dans la mesure où ils ont connaissance de la transmission de données par SWIFT, la loi sur la protection des données leur impose d'informer les personnes concernées. Ne donne suite aux exigences légales concernant la transparence du traitement des données que celui qui informe les personnes concernées d'un traitement subséquent de leurs données[8]. Eu égard à la chronologie d'un paiement, le devoir d'information ne peut incomber qu'au prestataire de services financiers qui relaie l'ordre.

De plus, la connaissance de la *seule possibilité* d'un accès de tiers aux données de SWIFT impose déjà un devoir d'informer. Pour cela, d'autres connaissances ne sont pas nécessaires, et elles n'existent manifestement pas. Même l'étude de la *Commission de la protection de la vie privée* n'a pas permis d'établir dans quelle mesure l'administration américaine a accès aux données des transactions SWIFT[9].

L'obligation de traiter les données en toute transparence subsiste. Que le public ait été informé de la transmission des données SWIFT aux autorités américaines ne joue en l'espèce aucun rôle. On ne peut pas affirmer qu'il est de notoriété publique, même après les révélations des médias, que SWIFT continue de retransmettre des données.

En revanche, il est établi depuis la publication du rapport de la commission belge[10] que SWIFT traite également ses données aux Etats-Unis. Dès lors, on se trouve confronté à une retransmission de données dans un pays dont la législation ne confère aucune protection des données équivalant à celle garantie par le droit suisse (art. 6, al. 1, LPD). Les prestataires de services financiers ne peuvent donc plus se prévaloir d'ignorer ce fait.

[8] L'exigence de transparence doit également être appréciée en regard du fait qu'il existe, dans le trafic des paiements internationaux, des solutions de rechange au système SWIFT. Cf. Rapport de la *CPVP*, p. 3.
[9] Cf. plus particulièrement le Rapport de la *CPVP*, p. 6.
[10] A plusieurs reprises, les médias avaient d'ailleurs déjà évoqué cet aspect.

IV. Conclusions

- A l'issue de son étude, la commission belge a constaté plusieurs entorses aux législations belge et européenne en matière de protection des données. Compte tenu de ses conclusions, il est établi que le droit suisse de la protection des données a également été violé. D'une part, on n'a pas prêté une attention suffisante à la transparence du traitement des données, et d'autre part les conditions énoncées à l'art. 6 LPD ne sont pas remplies.
- Nous nous rallions aux conclusions énoncées dans le rapport de *la Commission de la protection de la vie privée*. Une solution tenant compte à la fois de la lutte contre le terrorisme et des législations nationales en matière de protection des données inhérentes à chaque pays recourant au système SWIFT aurait dû faire l'objet de négociations. Du point de vue de la protection des donnés suisse, une telle nécessité perdure.
- Réclamer la transparence des prestataires de services financiers oeuvrant en Suisse ne suffit pas en regard de la situation globale. A l'instar de ce qui s'impose pour les données des passagers du trafic aérien, il convient d'améliorer la situation par voie de négociation: on devra trouver un arrangement qui satisfasse tant aux exigences de la législation américaine qu'aux normes européennes sur la protection des données.
- Nous apprécierions que les banques suisses appuient les efforts en ce sens par le biais de leurs représentants dans *le groupe de pays Suisse-Liechtenstein au sein de SWIFT*.
- Dans le cadre de notre coopération avec les autorités européennes chargées de la protection des données, notamment avec *le Groupe de travail «Article 29»* sur la protection des données, nous oeuvrerons en faveur d'une solution conforme aux normes de la protection des données, notamment aux exigences de l'art. 6 LPD.

4.2 Procédure interne à l'entreprise en cas de soupçon d'infraction au CP

Problématique

L'employeur est souvent confronté à la question de ses compétences en matière de gestion des preuves en cas d'infraction ou de soupçon d'infraction au Code pénal commise par l'employé au moyen d'Internet ou de l'E-mail. Un exemple qui revient fréquemment est celui représenté par l'employé soupçonné d'avoir communiqué par e-mail des secrets de fabrication à des tiers. L'employeur doit alors se demander, outre à comment préserver physiquement les preuves, s'il est lui-même en droit d'y accéder dans le but d'étayer son soupçon. La question est d'importance dans la mesure où des preuves collectées en violation de la personnalité peuvent être considérées comme inadmissibles par le juge.

Le secret des télécommunications (art. 43 de la loi sur les télécommunications, LTC, RS 784.10) et les normes de droit pénal concernant la violation de secrets privés (art. 179 Code pénal, CP, RS 311.0) n'étant pas applicables, la question se juge exclusivement à la lumière de la loi sur la protection des données (LPD, RS 235.1) et du droit du travail (art. 328, 328b et 362 Code des obligations, CO, RS 220).

Premièrement, il faut souligner que l'employeur, suite à son devoir de respecter la personnalité de l'employé à son poste de travail (art. 328 et 328b CO), n'a en principe pas le droit d'ouvrir ses e-mails privés. Le courrier de nature professionnelle reste par contre accessible à l'employeur en tout temps.

Dans des cas spécifiques, en particulier en présence de soupçons fondés d'infraction au Code pénal commis à l'aide de la messagerie électronique (p. ex. en cas de soupçon de violation du secret professionnel, art. 320 CP et art. 35 LPD), l'employeur est en droit de procéder à la préservation des preuves, c'est-à-dire à leur sécurisation par des mesures appropriées (en particulier, mais pas exclusivement, par l'établissement d'une copie physique à l'aide de backups ou du mirroring, c'est-à-dire la création d'une image identique des données originales grâce à un software conçu dans ce but).

Dans le présent contexte, il faut souligner que la préservation de preuves n'est légitime, c'est-à-dire justifiée par un intérêt prépondérant de l'entreprise, qu'en cas d'indices sérieux, notamment en présence de preuves ou au moins de soupçons concrets d'infraction au CP. De vagues sensations, impressions, suppositions ou un simple manque de confiance vis-à-vis d'un employé ne représentent en général pas un motif suffisant à justifier le déclenchement d'une enquête.

Il est indéniable qu'en pratique, il est difficile pour l'employeur de décider de l'opportunité de déclencher une enquête sur la base uniquement de soupçons, fussent-ils concrets. L'employeur est ainsi souvent amené à vouloir accéder aux e-mails privés de la personne soupçonnée, ou tout au moins à ceux jugées utiles à une confirmation du soupçon, afin de pouvoir décider en connaissance de cause de l'opportunité de déclencher une enquête. À noter ici qu'un tel accès pourrait, tout au moins en l'espèce, s'avérer intéressant aussi pour l'employé soupçonné. L'accès à ses e-mails privés pourrait éventuellement le libérer du soupçon et éviter une dénonciation (infondée ou mal fondée) à son encontre.

Sur la base de ce qui précède, l'employeur devrait pouvoir accéder aux contenus d'e-mails privés si l'accès était absolument nécessaire pour mieux fonder ou, au contraire, écarter un soupçon et si des intérêts prépondérants de la personne concernée ne s'y opposaient pas. À cette fin, la personne concernée devrait cependant être préalablement informée et donner son accord à l'employeur. Le principe des quatre yeux devrait aussi être respecté. Si la personne concernée devrait s'opposer à cette façon de procéder, nous vous recommandons de laisser aux autorités d'enquête la responsabilité centrale et unique de l'administration des preuves, en particulier de l'ouverture d'e-mails privés. Cela devrait garantir une enquête professionnelle et neutre, assurer l'intégrité des preuves grâce à des spécialistes (forensic computing scientists) ainsi que le respect du droit, en particulier les normes concernant la surveillance au lieu de travail (surtout art. 59, al. 1, lit. a, de la loi sur le travail, RS 822.11, ainsi que l'art. 26 de l'ordonnance 3 relative à la loi sur le travail, OLT 3, RS 822.113). Les preuves collectées par l'employeur en violation de ces normes de droit pourraient en effet être considérées comme inadmissibles par le juge.

Nous sommes également d'avis qu'à titre exceptionnel, si des intérêts prépondérants de l'employeur l'exigeaient (p. ex. en cas d'état de nécessité, article 34 CP) et si une mesure super-provisionnelle du juge ne suffisait pas à les sauvegarder, des preuves collectées par l'accès de l'employeur au contenu des mails privés de l'employé soupçonné pourraient être considérées comme admissibles.

Dans l'hypothèse où le droit cantonal devait prévoir la compétence unique des autorités d'enquête pour accéder aux e-mails privés, l'accord de l'employé y relatif ne pourrait rien y changer. L'inefficacité de la manifestation de volonté de l'employé résulterait non seulement de la nature prépondérante du droit public cantonal par rapport à un accord privé, mais aussi parce que un tel accord, du moins en l'espèce, pourrait porter atteinte à l'employé lui-même et donc être considéré aussi pour cette raison comme juridiquement non contraignant (voir les articles 362 et 328 CO).

4.3 Explications sur les systèmes d'accès électroniques aux domaines skiables

Des systèmes de plus en plus sophistiqués contrôlent l'accès aux domaines skiables et soulèvent des problèmes de protection des données. Alors qu'il y a quelques années, les sportifs étaient encore contrôlés par un système de cartes à perforer, ils le sont aujourd'hui par des systèmes électroniques. Le traitement de leurs données personnelles doit respecter les principes de la protection des données.

En achetant un abonnement qui lui donne accès aux installations sportives, le client doit fournir une photographie et des informations sur sa personne. Il s'agit de données personnelles. La collecte et l'utilisation de ces données par le propriétaire des installations constituent un traitement de données au sens de la loi sur la protection des données (LPD), dont les principes juridiques doivent être respectés. De plus en plus souvent, les exploitants d'installations de sports d'hiver recourent à des systèmes électroniques de contrôle d'accès, implantés à la station inférieure des remontées mécaniques. Lorsque l'usager franchit le portillon, la photo du détenteur de l'abonnement apparaît sur un écran. Le système permet d'une part de contrôler si le détenteur et le porteur de l'abonnement sont bien une seule et même personne, et d'autre part de vérifier la validité de l'abonnement. Généralement, le contrôle est effectué par le personnel de la station, mais dans certains domaines skiables, l'écran est également visible pour des tiers qui se trouvent à proximité du point de contrôle. Les données personnelles du détenteur de l'abonnement apparaissent à l'écran et y restent visibles jusqu'au passage du client suivant, ce qui peut durer plusieurs minutes.

Le PFPD rappelle que toute personne a un droit au respect de sa sphère privée et notamment de son identité à l'égard de tiers, y compris justement dans le cadre de ses loisirs. Quiconque traite des données personnelles doit s'appuyer sur d'un motif justificatif: ce peut être une loi, mais également un intérêt privé ou public prépondérant, ou encore le consentement des personnes concernées. Même lorsqu'il existe un motif justificatif, les principes généraux de la protection des données s'appliquent (conformité au but, bonne foi, proportionnalité); notamment, selon le principe de la transparence, l'information du détenteur de l'abonnement sur le but et les modalités du traitement de ses données personnelles est nécessaire.

Cela étant, l'exploitant d'une station de sports d'hiver peut-il faire valoir un motif justificatif pour l'affichage à l'écran de données personnelles également visibles pour des tiers? En d'autres termes, un tel affichage est-il licite au sens de la LPD? Le PFPD

souligne qu'aucune loi ne s'applique au cas présent, et aucun intérêt public ne peut être invoqué. Ne restent dès lors, à titre de motifs justificatifs, qu'un intérêt privé prépondérant ou le consentement des personnes concernées.

Certes, l'exploitant d'une station de sports d'hiver a un intérêt légitime, et en principe prépondérant, à vérifier la validité des abonnements, et notamment à contrôler que des tiers n'utilisent pas abusivement des abonnements non transmissibles. A cette fin, il a le droit d'installer des systèmes électroniques de contrôle d'accès, tout en respectant les principes généraux de la protection des données. Sous cet angle, les réflexions suivantes sont décisives:

- le PFPD doute que l'affichage public à l'écran soit utile au contrôle de la validité des abonnements. Il ne revient pas aux autres clients de contrôler, en lieu et place du personnel, qu'aucun abus n'est commis. Il semble plutôt que le recours à de tels systèmes ait pour objectif de dissuader d'éventuels resquilleurs;
- dans toute la mesure du possible, il convient d'appliquer la mesure qui préservera le plus la sphère privée (principe de la proportionnalité). L'affichage public de données personnelles peut signifier une intrusion non négligeable dans la sphère privée des personnes concernées. Dans le cas présent, une telle mesure ne respecte pas le principe de la proportionnalité, car il existe d'autres moyens de contrôle à la fois efficaces et conformes aux impératifs de la protection des données, par exemple les contrôles systématiques ou ponctuels par des employés. De plus, seul le personnel doit avoir accès aux écrans;
- enfin, il faut tenir compte du fait qu'en cas d'abus, ce ne sont pas les données personnelles du porteur qui s'affichent, mais celles du détenteur de l'abonnement qui n'a pas forcément connaissance de l'abus et est ainsi injustement stygmatisé.

Les exploitants d'installations de sports d'hiver ne peuvent donc pas non plus invoquer un intérêt privé prépondérant à l'affichage public de données personnelles. Le seul motif justificatif restant est donc le consentement des personnes concernées. A cet égard, le PFPD souligne que ce consentement doit être donné librement et en toute connaissance de cause. En d'autres termes, le client doit pouvoir s'opposer au traitement de ses propres données sans qu'il en résulte pour lui un désavantage quelconque. La communication des données personnelles devrait alors être facultative, ce qui serait techniquement possible mais contrarierait les intentions de contrôle de l'exploitant.

En conclusion, on peut affirmer que l'affichage de la photographie et de l'identité des usagers d'installations de sports d'hiver est incompatible avec la loi fédérale sur la protection des données. D'autres moyens, plus respectueux de la sphère privée, permettent de vérifier la validité des abonnements et d'éviter les abus, par exemple les contrôles systématiques ou sporadiques tels que les connaissent les transports en commun. Dans ces conditions, la communication de données personnelles à des tiers n'est pas nécessaire et est disproportionnée.

En cas d'atteinte illicite à la personnalité, les personnes concernées peuvent déposer plainte en vertu de l'art. 15 LPD.

4.4 Déclaration de Londres

«Communiquer sur la protection des données et la rendre effective»

Origine de cette initiative

Cette initiative repose sur le discours prononcé par Alex Türk, Président de l'autorité française de protection des données, lors d'une conférence organisée à Varsovie en mai 2006 par l'Inspecteur Général à la Protection des Données polonaise, sur le thème «Sécurité publique et protection des données». Dans ce discours, Alex Türk exprimait sa vive préoccupation face aux défis auxquels sont actuellement confrontées les autorités de protection des données dans le monde. Il insistait sur la nécessité absolue que les autorités infléchissent leur action pour répondre à ces défis, si l'on ne veut pas voir la philosophie qui sous-tend les règles de protection des données privée de sa substance.

A la suite de cette conférence, le Contrôleur européen a invité la CNIL à développer une initiative commune exposant l'urgence d'une nécessaire action et visant à provoquer une prise de conscience collective, qui serait présentée à la conférence internationale de Londres. L'Information Commissioner britannique a immédiatement soutenu cette initiative. Ce texte a été rédigé en étroite collaboration entre ces trois autorités.

En adhérant à cette initiative, les autorités participantes s'engagent à coordonner leurs actions pour contribuer à cette prise de conscience, notamment en:

- accentuant leurs activités de communication, sur la base d'idées communes, dont certaines sont évoquées dans le texte ci-joint;
- adaptant leurs pratiques et méthodes de travail, grâce à l'évaluation de leur efficacité et au renforcement de leurs capacités d'expertise, de prospective et d'intervention dans le champ technologique;
- contribuant à faire reconnaître l'action de leurs autorités de manière institutionnelle, sur le plan international et à promouvoir l'implication de tous acteurs appropriés sur les plans national et international.

A l'heure actuelle, les autorités de protection des données suivantes ont en principe apporté leur soutien à cette initiative:

- Commission nationale de l'informatique et des libertés (France)
- Contrôleur européen à la protection des données (Union Européenne);
- UK Information Commissioner (Royaume-Uni);
- Commissaire fédéral à la protection de la vie privée (Canada);
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Allemagne);
- Agencia Española de Protección de Datos (Espagne);
- Garante per la Protezione dei Dati Personali (Italie);
- College Bescherming Persoonsgegevens (Pays-Bas);
- Privacy Commissioner (Nouvelle Zélande);
- Préposé fédéral à la protection des données et à la transparence / Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Suisse).

Cette initiative conjointe sera présentée lors de la session fermée de la conférence internationale des commissaires à la protection des données, qui se tiendra à Londres les 2 et 3 novembre prochains. Elle ne sera pas présentée pas la forme d'une résolution. Elle sera présentée comme une initiative conjointe de la CNIL, du Contrôleur européen et du UK Information Commissioner, que soutiennent les différentes autorités mentionnées plus haut, qui se seront engagées à adapter leurs actions en conséquence. Les autres autorités présentes à la Conférence seront invitées à exprimer leur soutien, voire à se rallier à cette initiative si elles le souhaitent. Il n'est pas prévu que ce document soit formellement adopté par la conférence.

Après avoir rappelé pourquoi la protection des données est indispensable à une société (I), ce texte analyse dans le détail les risques qui pèsent aujourd'hui sur les libertés individuelles et la protection des données dans le monde, et qui représentent autant de défis pour les autorités de contrôle (II). Il tire de ce constat différentes propositions d'actions et d'initiatives coordonnées (III), ainsi que le développement d'une nouvelle stratégie commune de communication (IV).

I. LA PROTECTION DES DONNEES EST INDISPENSABLE A UNE SOCIETE

1. La protection des données personnelles de nos citoyens est un impératif vital pour une société, au même titre que la liberté de la presse ou la liberté d'aller et venir. Nos sociétés sont de plus en plus dépendantes des nouvelles technologies, et les données à caractère personnel sont collectées ou générées dans des proportions sans cesse plus importantes. Il en devient d'autant plus essentiel que les libertés individuelles et les autres intérêts légitimes des citoyens soit respectés de manière adéquate dans les traitements de l'information.

2. La protection des données n'est pas, ne doit pas être conçue comme un thème abstrait, théorique, voire même «théologique». Les règles de protection des *données* protégent des *personnes.* Il s'agit de protéger un droit à ne pas être fiché, surveillé, contrôlé de manière abusive et incontrôlée; il s'agit de protéger la dignité humaine, de permettre aux personnes d'exercer leurs droits et que leurs intérêts légitimes soient préservés.

3. La protection des données ne peut être une réalité que si les règles de protection des données sont respectées en pratique. Les autorités de protection des données jouent un rôle fondamental à cet égard. Cependant elles ne joueront ce rôle qu'en communiquant de manière efficace sur la protection des données, en impliquant les acteurs concernés, et si nécessaire en faisant usage de leurs pouvoirs de contrôle et de mise en œuvre.

II. DEUX VAGUES; UN TRIPLE DEFI

4. Les libertés individuelles et nos autorités sont exposées à des risques sans précédents; elles sont menacées de manière irréversible par deux vagues, et doivent faire face à un triple défi.

A. Le premier défi est d'ordre technologique, du fait d'une combinaison de facteurs

5. **Le facteur «accélération»**: Internet, RFID, nanotechnologies, etc. Les autorités ne sont pas hostiles au progrès technologique. Mais les délais entre la découverte d'un phénomène et sa mise en œuvre technologique se raccourcissent et le temps de passage d'une innovation à une autre innovation, du développement d'un prototype à son déploiement industriel, se réduit sans cesse. Il devient de plus en plus difficile de faire coïncider l'adaptation ou l'interprétation des règles de droit à l'évolution technologique: le temps technologique accélère sans cesse, tandis que le temps juridique reste particulièrement lent, régi par le rythme des procédures démocratiques.

6. **Le facteur «globalisation»**: les délocalisations de traitements de données sont en plein essor. Il est indéniablement devenu extrêmement difficile, sur le plan international, de contrôler les échanges de données. Cette tendance à la globalisation est souvent en conflit avec une grande caractéristique de la règle de droit, à savoir un champ d'application étroit, limité à un territoire et à un champ de compétence ordonné et balisé.

7. **Le facteur «ambivalence»**: l'innovation technologique est porteuse de progrès comme de dangers. Autant les individus sont tentés par le confort qu'elle procure, autant ils sont peu conscients des risques qu'elles comportent, du moins jusqu'à ce qu'ils en soient victimes ou qu'il soit trop tard: ils ne se préoccupent pas de leur traçabilité, de la surveillance potentielle de leurs déplacements, de leurs comportements, de leurs relations. Cette ambivalence de la technique est difficile à concilier avec la règle juridique qui doit, par définition, être univoque, et se trouve, bien souvent, en inadéquation avec cette ambivalence du progrès technique.

8. **Le facteur «imprévisibilité»**: les usages de la technologie se développent souvent de manière imprévisible, y compris parfois pour leurs concepteurs. Les usages imprévus d'une technologie peuvent, de ce fait, être difficiles à encadrer, surtout quand ils divergent des usages pour lesquels celle-ci avait été initialement conçue, et pour lesquels la loi semblait en mesure de s'appliquer.

9. **Le facteur «invisibilité» (Invisibilité virtuelle/Invisibilité physique ou réelle)**: Le traitement de l'information est de plus en plus «invisible», impalpable, de moins en moins maîtrisable. La technologie tend à devenir invisible non seulement du fait de plus en plus de traitements de données virtuels sont réalisés à l'insu des personnes (traçabilité des déplacements physiques dans les transports en commun, des consultations sur Internet, des communications téléphoniques, etc.): c'est l'invisibilité virtuelle, liée aux processus. Elle tend aussi à devenir invisible du fait de son extrême miniaturisation: c'est l'invisibilité physique ou réelle. Dans quelques années, avec les nanotechnologies, il sera devenu impossible de voir à l'œil nu que la technologie est présente dans un objet: comment encadrer et contrôler des traitements effectués par le recours à une technologie invisible?

10. **Le facteur «irréversibilité»**: Le progrès technologique est irréversible: nous ne vivrons plus jamais dans un monde sans ordinateurs, sans Internet, sans téléphones portables, sans identification biométrique, sans géolocalisation, sans vidéosurveillance. Ces technologies tendent au contraire à s'imbriquer les unes dans les autres, et les synergies qu'elles créent sont des plus dangereuses pour nos sociétés.

B. Le second défi est d'ordre normatif, lié aux nouvelles législations de lutte antiterroriste

11. Le développement des législations anti-terroristes lance un défi aux autorités de protection des données qui, dans ce contexte, doivent éviter les pièges, dénoncer les illusions et combattre les mythes.

12. **Le piège du manichéisme:** ni législateur, ni juridiction, ni association militante, les autorités indépendantes de protection des données ont un rôle très particulier à jouer. Il leur sera rarement possible de résoudre un problème de manière tranchée, «blanc ou noir». Ainsi, l'ensemble des autorités de protection des données reconnaît la légitimité des politiques de lutte anti-terroriste mises en œuvre depuis quelques années. Mais elles doivent également, conformément aux missions qui leur ont été confiées par les textes fondateurs, et au nom de la société, rechercher en permanence un équilibre entre les impératifs de sécurité publique, d'une part, et les exigences de la protection de la vie privée et des données personnelles, d'autre part. Elles doivent assumer ce rôle en toute indépendance, et rejeter les accusations inacceptables d'irresponsabilité qui sont parfois portées à leur égard en la matière.

13. **Le risque de l'engrenage:** ce risque est le suivant. Le législateur crée une base de données à un moment donné, dans des circonstances données. L'autorité de contrôle est associée à son développement. Ultérieurement, le législateur envisage d'étendre le périmètre de cette base – par exemple en étendant d'abord catégories de personnes concernées, puis les motifs d'inscription dans le fichier, puis enfin les catégories de personnes pouvant le consulter… Les promoteurs de ces modifications ultérieures font valoir à l'autorité qu'elle ne peut s'opposer à une simple extension, puisqu'elle a accepté le principe de la création du fichier de base, et ainsi de suite si nécessaire… Ainsi, entre la première et la dernière étape du développement d'un fichier, il se sera opéré un glissement qui remettra fondamentalement en question l'équilibre acceptable de son périmètre d'origine.

14. **L'illusion de «l'exemplarité»**: les exécutifs nationaux invoquent souvent le fait que d'autres pays ont déjà mis en place un dispositif pour reprocher aux autorités de contrôle de tel ou tel pays leur réticence à l'accepter sans discuter. Cela pose de réels problèmes d'harmonisation et rend nécessaire de recourir à des raisonnements fondés sur la définition de dénominateurs communs.

15. **Le mirage du fichier «remède miracle»:** les autorités doivent rappeler sans cesse au public et aux exécutifs que la création d'un fichier informatique comportant toujours davantage de données ne règle pas tout. Il faut désacraliser le caractère supposé infaillible du fichier informatique. Quand de plus en plus de données personnelles sont enregistrées, les risques d'identification erronée, de données périmées et autres erreurs augmentent. Ceci peut causer de véritables préjudices aux personnes, que ce soit pour leur santé, la possibilité d'effectuer des choix de vie, leur prospérité, voire même leur liberté.

16. **Le mythe du fichier infaillible (la problématique «majorité/minorité»)**: il est trop souvent supposé - à tort - que les personnes enregistrées dans une base de données le sont pour une raison valable. Il en résulte que les personnes qui figurent dans ces fichiers de manière indue («la minorité») se retrouvent dans une situation parfois dramatique, car tout portera à croire qu'il est impossible d'être dans ce fichier, aussi performant technologiquement, sans que cela soit justifié. Ainsi il est indispensable, sur le plan éthique, de continuer à affirmer que l'informatique peut être faillible et de proscrire la prise de décision automatisée, tout particulièrement dans des domaines comme la sécurité ou la justice.

C. Le troisième défi est celui de la réputation de la protection des données

17. Au moins dans un certain nombre de pays, la protection des données et les autorités de protection ne jouissent pas de la réputation positive qu'elles méritent. Les règles de protection des données peuvent être perçues comme complexes et difficiles à appliquer de manière cohérente, prévisible et réaliste. D'autres critiquent les règles de protection des données comme trop abstraites, et pas assez recentrées sur les dommages réels ou supposés – causés aux personnes ou à la société dans son ensemble – si ces règles ne sont pas observées. D'autres encore critiquent la manière dont ces règles sont interprétées ou mises en œuvre, ce qui les dissuade de se mettre en conformité ou d'investir dans des efforts de mise en conformité. De telles perceptions négatives peuvent être celles d'hommes politiques, d'administrations, d'entreprises, des médias mais aussi de particuliers. Il est nécessaire de combattre ces perceptions, en démontrant l'importance pratique de la protection des données, en matérialisant la réalité des droits et libertés fondamentaux, et en reconsidérant certaines pratiques, si cela s'avère nécessaire.

III. LIGNES D'ACTION ET INITIATIVES POUR LES AUTORITES DE PROTECTION DES DONNEES

18. Devant la gravité des risques énoncés ci-dessus, les autorités de protection des données doivent, de manière urgente, se donner les moyens de provoquer une prise de conscience collective quant aux risques de destruction irréversible qui menacent les libertés individuelles dans leurs pays. Elles doivent aussi évaluer leurs méthodes de travail et améliorer leur efficacité.

A. Les autorités doivent ensemble proposer des réformes et desstratégies coordonnées pour agir mieux, plus efficacement et de manière plus ciblée

19. **Développer la capacité d'expertise, de prospective et d'intervention dans le domaine technologique:** la protection des données «souffre» au-jourd'hui de son image excessivement juridique; or la crédibilité de nos institutions est et sera de plus en plus liée à notre capacité à comprendre et à anticiper les développements technologiques.

20. Pour analyser ces nouveautés, nos autorités doivent élaborer des stratégies de division du travail en fonction des enjeux, des expériences, des responsabilités, des moyens qui sont les leurs.

21. Elles doivent réfléchir aux relations qu'elles souhaitent entretenir avec chercheurs et industriels dans le domaine des technologies de l'information et de communication. Elles doivent présenter aux entreprises et aux administrations la valeur de la protection des données et les bénéfices qu'elles peuvent en attendre.

22. **Évaluer notre efficacité et adapter nos pratiques:** il est absolument nécessaire de procéder à une évaluation sans fard de l'efficacité respective de nos autorités. Notre action a-telle un impact réel, faisons-nos une différence en pratique? Les mots se traduisent-ils par une réalité? De telles évaluations nous permettront de tirer des leçons pour améliorer nos résultats.

23. L'évaluation de l'efficacité de nos autorités mènera sans doute certaines autorités à revendiquer que le législateur les dote de pouvoirs dont elles ne disposeraient pas. Elle pourra aussi remettre en cause des pratiques de fonctionnement au sein de nos autorités. Celles-ci doivent concentrer leur action prioritairement sur les principaux risques existants aujourd'hui, et veiller à ne pas être d'une rigidité excessive sur des sujets qui ne le méritent pas. Elles doivent être prêtes à faire preuve de davantage de pragmatisme et de souplesse.

B. Les autorités doivent réfléchir ensemble pour faire reconnaître leur action de manière institutionnelle sur le plan international et impliquer d'autres acteurs

24. **Une nécessaire structuration de la Conférence Internationale:** la Conférence Internationale des Commissaires à la Protection des Données doit devenir le fer de lance de l'action de nos autorités sur le plan international. Il faut en assurer la viabilité, en améliorer le fonctionnement, la rendre plus visible et plus efficace, la faire vivre au long de l'année, élaborer un plan d'action, un programme de communication. Ceci impliquera sans doute de réfléchir à la création d'un secrétariat permanent. La conférence doit devenir, sur le plan international, un acteur incontournable dans le traitement d'initiatives internationales ayant une incidence sur le droit de la protection des données; elle doit permettre la discussion et la remontée d'idées concrètes, afin de mieux suivre les développement internationaux, d'harmoniser les pratiques et d'adopter des positions communes.

25. **Elaboration d'une Convention Internationale:** par la déclaration de Montreux, les Commissaires à la protection des données appelaient au développement d'une Convention universelle de protection des données. Cette initiative doit être soutenue auprès des institutions compétentes par nos autorités, dans le respect de leur positionnement institutionnel et, si nécessaire, après coordination entre autorités compétentes au niveau national. Nos autorités doivent promouvoir cette initiative dans leurs sphères d'influence respectives, en particulier au sein des organisations régionales ou des zones linguistiques auxquelles elles appartiennent. Il pourra s'avérer nécessaire de développer des solutions globales pour le respect de la protection de la vie privée et des données personnelles dans des domaines spécifiques (ex: gouvernance de l'Internet; transactions financières; transport aérien); ces questions devront être traitées par les autorités par tous moyens appropriés.

26. **Participation d'autres acteurs (société civile; ONG):** d'autres acteurs de la protection des données et de la vie privée sont aujourd'hui actifs, sur le plan national comme sur le plan international, à différents niveaux et dans différents secteurs. De telles organisations pourraient être des partenaires stratégiques et contribuer de manière substantielle à l'amélioration de l'efficacité de nos autorités. La coopération avec d'autres acteurs doit ainsi être encouragée, parfois même activement développée.

IV. POUR UNE NOUVELLE STRATEGIE DE COMMUNICATION

27. La communication est un facteur clé pour rendre la protection des données plus effective. Un message qui n'est pas reçu ou reste incompris est un message inutile. Un avis ou une décision qui n'est pas accessible aura un impact limité et ne vaudra pas les efforts nécessaires à le développer.

A. Nous devons, de manière urgente, concevoir et mettre en œuvre une nouvelle stratégie de communication, sur le plan national et sur le plan international

28. **Un objectif: communiquer.** Une meilleure communication vers le public doit être un objectif prioritaire de nos autorités. Il n'est pas concevable que dans certains de nos pays où l'on inscrit le droit à la protection des données parmi les droits fondamentaux imprescriptibles tels que la liberté d'aller et venir ou la liberté de la presse, l'immense majorité de nos concitoyens n'ait aucune conscience d'en être titulaires, ni de leur importance. Ceci est d'autant moins acceptable que la protection des données peut même avoir une réputation négative.

29. Nous devons nous engager dans un puissant effort de pédagogie, et à long terme, visant à informer les personnes de l'existence et du contenu de ces droits. L'effet de ces actions doit être mesurée. Deux catégories doivent être visées en priorité:

    - Les élus nationaux et locaux qui ont, par nature, une responsabilité particulière en la matière et dont l'information doit être améliorée;
    - Les jeunes générations qui font preuve d'une grande indifférence vis-à-vis de ces questions tant ils sont habitués à manipuler ces nouvelles technologies. Il faut donc agir dans le secteur éducatif le plus tôt possible.

30. **Un levier d'action: communiquer. I**l est important et urgent de doter les Autorités de meilleurs moyens d'action et de leur assurer une reconnaissance sur le plan international. La confiance et le soutien du public sont absolument essentiel. La protection des données doit être rendue plus concrète. Seules les organisations communiquant de manière compréhensible, accessible et parlante au grand public, généralement via les médias, disposeront de la puissance nécessaire pour influencer les opinions publiques, et donc pour être entendues et prises au sérieux par les Etats et la communauté internationale. C'est à cette condition qu'ils pourront obtenir ces moyens d'action indispensables.

31. Ceci passe par une professionnalisation de la fonction de la communication au sein de nos autorités, et par le fait que les messages de communication émis par nos autorités soient cohérents entre eux.

B. Une piste intéressante consisterait à reprendre dans nos activités de communication la notion de capital à réserer, par analogie avec le thème du capital naturel de notre planète mis en danger par la pollution issue de l'activité humaine

32. De même qu'on ne peut pas agir impunément en matière de protection de l'environnement, nous devons être extrêmement vigilants dans notre domaine, à l'égard de toute avancée technologique non maîtrisée comme de toute mise en œuvre de normes nouvelles consenties plus ou moins consciemment, parce que ce capital de garantie de nos libertés et de notre identité peut alors être amputé ou menacé dans son existence même. Et il ne se renouvellera pas, précisément en raison du phénomène d'irréversibilité des effets du progrès technologique.

33. La protection des données est peut-être aussi précieuse que l'air que nous respirons. Tous deux sont invisibles, mais les conséquences sont tout aussi désastreuses quand ils viennent à manquer.

V. PROGRAMME D'ACTIVITES DE SUIVI

34. La discussion de cette initiative lors de la session fermée de la conférence internationale des commissaires à la protection des données et à la vie privée de Londres doit être la première occasion d'élaborer un consensus sur la nécessité d'une action, sur le développement de moyens pour une meilleure communication, et pour faire en sorte que la protection des données soit une réalité.

35. Les autorités soutenant cette initiative s'engagent à participer, et si nécessaire à être responsable d'un certain nombre d'activités communes, telles que:

- Un atelier sur les questions stratégiques: conditions pour rendre la protection des données plus effective; développement éventuel de principes de «bonne supervision» en matière de protection des données; information sur les bonnes pratiques; réflexion sur le développement d'une convention internationale (commissaires et services);
- Un atelier sur la communication: expertise disponible en matière de communication sur la protection des données (ex: campagnes média; enquêtes d'opinion); développement d'un message commun et d'outils pour le répandre (responsables communication);

- Un atelier sur la mise en œuvre des règles de protection des données: expertise disponible pour s'assurer du respect des règles et le contrôler; moyens efficaces d'inspection - y compris audits - et d'intervention (commissaires et services des contrôles);
- Un atelier sur l'organisation interne des autorités: expériences récentes en matière de changement organisationnel; projets d'amélioration de l'efficacité de l'autorité (commissaires et services en charge de l'organisation de l'autorité)
- Toute autre activité pertinente pour cette initiative.

4.5 Résolution relative aux modalités pratiques d'organisation de conférence

28ème Conférence internationale des commissaires à la protection des données et de la vie privée Londres, 3 novembre 2006

Proposée par: Privacy Commissioner, Nouvelle Zélande

Soutenue par:

- Privacy Commissioner, Australie
- Privacy Commissioner for Personal Data, Hong Kong
- Information Commissioner, Royaume Uni
- Commissaire fédérale à la protection de la vie privée du Canada
- Préposé fédéral à la protection des données, Suisse
- Information and Privacy Commissioner, Colombie britannique, Canada
- Controleur européen de la protection des données, Union européenne
- Data Protection Commissioner, Irlande
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Allemagne
- Commission de la protection de la vie privée, Belgique
- Commission nationale de l'informatique et des libertés, France
- Generalny Inspektor ochrony danych osobowych, Pologne

Résolution

La 28ème Conférence internationale des commissaires à la protection des données et de la vie privée adopte la résolution d'instituer un groupe de travail afin de:

(a) Préparer un document recensant les modalités existantes d'organisation de la conférence et les attentes de la conférence envers son hôte

(b) Explorer les idées permettant d'améliorer les arrangements existants quant à l'organisation de la conférence, afin de garantir une viabilité constante des conférences annuelles et de promouvoir leur amélioration de manière continue et de proposer des recommandations à la 29ème Conférence.

Exposé des motifs

La Conférence internationale des commissaires à la protection des données et de la vie privée entre dans sa troisième décennie. Elle progresse de manière constante tant en terme de participation que de qualité. La nécessité d'une coopération efficace entre les autorités de protection des données est plus que jamais reconnue et la conférence a un rôle déterminant à jouer à cet égard.

La conférence devrait avoir un avenir brillant et prometteur. Pourtant, sur les sept années écoulées une conférence s'est conclue sans qu'aucune autorité ne se soit proposée pour organiser la conférence suivante et, à deux reprises, les hôtes ont retiré leur proposition.

Il est aujourd'hui opportun d'initier une réflexion sur les modalités d'organisation de la conférence qui tienne compte de la croissance du nombre de ses participants. C'est d'ailleurs l'occasion de reprendre des travaux antérieurs en la matière. Par exemple, en 1996 une enquête a été menée auprès des participants concernant les futures orientations de la conférence, qui a abouti à la rédaction d'un «document d'options». La conférence a, à plusieurs reprises, réfléchi sur certains aspects de son organisation et permis de dégager un consensus sur ceux-ci. Elle a également mis en place une procédure d'accréditation la dotant de bases saines pour aller de l'avant.

La résolution prévoit qu'un groupe de travail soit créé pour étudier ce problème et formuler des propositions construites à la conférence. La résolution se distingue en deux parties.

Recenser les arrangements existants

La résolution propose tout d'abord que le groupe de travail recense, de manière général, les arrangements existants en matière d'organisation. Il pourrait ainsi rassembler, en un endroit unique et accessible, les décisions que la conférence a précédemment adoptées relatives, par exemple, aux frais d'inscription, au statut d'observateur et à la sélection des hôtes de la conférence trois ans à l'avance. Il pourrait se pencher sur plusieurs questions tels que le mois d'organisation de la conférence, les questions de traduction et le processus de sélection des futurs hôtes. Outre l'intérêt pratique que revêtirait un tel guide pour les futurs hôtes, il constituerait également une base utile pour formuler toutes propositions de modification des arrangements actuels.

Il serait préférable d'exclure des missions de ce groupe de travail les procédures d'accréditation des autorités et d'adoption des résolutions des travaux du groupe, dans la mesure où ces aspects ont d'ores et déjà fait l'objet de travaux récents et détaillés.

Explorer des pistes de changement

Le groupe de travail explorerait toutes idées d'amélioration des arrangements organisationnels existants. Au regard de l'expérience de cette année, il est essentiel de réfléchir aux actions à mener pour assurer la viabilité des conférences annuelles. Peut-être la procédure d'identification et de sélection des hôtes nécessiterait-elle d'être bien définie plutôt que de traiter cette question rapidement lors de la session fermée de la conférence. Ceci pourrait inclure, par exemple, la circulation d'«offres» d'accueil de la conférence à l'avance, sur le modèle de la procédure d'adoption de résolutions. Un comité exécutif devrait peut-être être créé qui prenne les mesures nécessaires pour assurer un programme d'accueil de la conférence dans l'avenir. D'autres options pourraient être identifiées par le groupe.

Le groupe de travail pourrait également réfléchir à d'autres suggestions d'amélioration des modalités d'organisation de la conférence. Par exemple, serait-il possible de collecter et de répondre au mieux aux attentes des autorités participantes quant à l'organisation de la conférence? Le recours à des comités de programme et à des enquêtes de satisfaction serait-il utile? La conférence peut-elle faciliter le transfert d'expérience d'un hôte à l'autre?

A ce stade le groupe devrait recueillir les idées des participants et travailler de nouveau sur les options qui ont déjà pu être proposées à la conférence, mais qui n'ont pas encore été mises en œuvre (telle que le document d'option de 1996 et la proposition de déclaration de Montreux relative à la création d'un site Web permanent de la conférence).

4.6 Résolution sur La protection de la vie privée et les moteurs de recherche[1]

28ème Conférence internationale des commissaires à la protection des données et de la vie privée dondres, Royaume-Uni, 2 et 3 novembre 2006

Auteur: Commissaire à la protection des données et à l'accès à l'information du Land de Berlin, Allemagne

Cosignataires: Allemagne (Commissaire fédéral à la protection des données et à l'accès à l'information), Irlande (Data Protection Commissioner), Nouvelle–Zélande (Privacy Commissioner), Norvège (Datatilsynet), Pologne (General Inspector for Personal Data Protection)

Résolution[2]

Aujourd'hui, les moteurs de recherche sont devenus les clefs pour accéder au 'cyberespace' afin de trouver de l'information sur l'Internet. Ils sont ainsi devenus des outils indispensables. L'importance croissante des moteurs de recherche pour trouver de l'information sur Internet mène à des intrusions considérables dans la vie privée des utilisateurs.

[1] Cette résolution ne traite pas de fonctions de recherche offertes par des fournisseurs de contenus pour leurs propres sites Web. L'utilisation du terme „moteur de recherche" dans cette résolution se rapporte à la fourniture d'un service aux fins de localisation de ressources sur Internet, sur la base de mots-clés de recherche définis par l'utilisateur et opérant à travers différents sites Web.
[2] Cette résolution ne traite pas des questions soulevées par les pratiques de nombre de moteurs de recherche qui stockent et publient des copies du contenu de sites Web, y compris des données personnelles publiées sur ces sites, légalement ou illégalement („caching").

Les fournisseurs de moteurs de recherche ont la capacité de reconstituer un profil détaillé des intérêts de leurs utilisateurs[3]. De nombreux logs IP permettent d'identifier les utilisateurs, particulièrement quand ils sont combinés avec les données stockées par ailleurs par les fournisseurs d'accès. L'utilisation de moteurs de recherche étant de nos jours pratique commune chez les internautes, les données de connexion stockées par les fournisseurs des grands moteurs de recherche permettent d'établir un profil détaillé des intérêts, des idées et des activités, et ce, à travers différents secteurs (par exemple des données relatives à des activités professionnelles, aux loisirs, mais aussi des données particulièrement sensibles comme par exemple celles relatives à des opinions politiques, des croyances religieuses, ou même des préférences sexuelles).

Les Commissaires à la protection des données et à la vie privée se sont particulièrement inquiétés, dans le passé, de la possibilité de constituer des profils de citoyens[4]. Aujourd'hui, la technologie disponible sur Internet rend cette pratique, dans une certaine mesure, techniquement possible, et ce sur le plan mondial.

Il est clair que ces informations peuvent permettre d'identifier les personnes. Cette faculté est utile pour les fournisseurs de moteurs de recherche eux-mêmes, mais également à des organismes tiers. Ainsi, un exemple récent à mis en valeur l'intérêt que portent les organismes chargés de faire respecter la loi sur ces informations: au printemps 2006, le Ministère de la Justice des États-Unis a demandé à Google, Inc. de lui fournir des millions de requêtes d'utilisateurs, dans le cadre d'une action en justice relative, entre autres, à la protection contre la pornographie enfantine en ligne. Google a refusé de se soumettre à cette injonction et a finalement remporté cette bataille judiciaire. Ultérieurement, AOL a publié une liste de près de 20 millions de requêtes faites par environ 650,000 utilisateurs d'AOL sur le moteur de recherche d'AOL au cours d'une période de trois mois, dont il était prétendu qu'elles étaient anonymes. D'après la presse, cependant, il était possible d'identifier des utilisateurs particuliers en combinant le contenu de leurs requêtes. Cette liste a été rapidement retirée par AOL qui avait alors reconnu avoir commis une erreur. Dans l'intervalle, cependant, elle avait apparemment déjà été téléchargée et diffusée de maintes fois sur Internet. De plus, un certain nombre de sites l'avait publiée sous un format plus facilement exploitable aux fins de recherche.

[3] A noter que dans certains cas ceci est fait à l'aide de cookies persistants.

[4] Voir par exemple la Position commune adoptée par le groupe de travail international sur la protection des données dans le secteur des télécommunications sur la protection de la vie privée et les moteurs de recherche (adoptée en premier lieu à la 23ème réunion à Hong Kong SAR, Chine, le 15 avril 1998; revue et mise à jour à la 39ème réunion, 6-7 avril 2006, Washington D.C.); http://www.datenschutz-berlin.de/doc/int/iwgdpt/search_engines_en.pdf. Voir également le chapitre 5 ('surfer et chercher') du document de travail adopté par le Groupe dit «de l'article 29» - document WP12:' Le respect de la vie privée sur Internet - Une approche européenne intégrée sur la protection des données en ligne2 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp37fr.pdf

Il doit être rappelé que tant les données de connexion que le contenu de requêtes effectuées sur des moteurs de recherche peuvent constituer des données à caractère personnel.

Ces affaires soulignent que les «historiques de recherches» stockés par les fournisseurs de moteurs de recherche constituent d'ores et déjà des données relatives à des personnes identifiables dans de nombreux cas. En particulier, dans les cas où les opérateurs de moteurs de recherche offrent d'autres services permettant l'identification d'un individu (par exemple de courrier électronique), le trafic et le contenu des requêtes peuvent être combinés avec d'autres informations personnellement identifiables en provenance de ces autres services pendant une seule session (par exemple sur la base d'adresses IP). Il est probable qu'à l'avenir le pourcentage des données d'«historiques de recherche» pouvant être attribuées à des personnes augmentera en raison de l'utilisation de numéros IP fixes dans les services DSL ultra-rapides ou d'autres connexions à haut débit, dans le cadre desquels les ordinateurs de l'utilisateur sont „toujours connectés". Il augmentera encore davantage quand l'introduction d'IPV6 sera achevée.

Recommandations

La conférence internationale demande aux fournisseurs de moteurs de recherche qu'ils respectent les règles de base de protection des données personnelles et de la vie privée, telles que fixées dans les lois nationales de nombreux pays, ainsi que dans des documents de politique publique et traités Internationaux (par exemple les principes directeurs de l'ONU, les Lignes directrices sur la protection de la vie privée de l'OCDE, la Convention 108 du Conseil de l'Europe, le cadre concernant la vie privée de l'APEC et les directives de la protection de données et de la vie privée de l'Union Européenne) et qu'ils modifient leurs pratiques comme suit:

1. Entre autres, les fournisseurs de moteurs de recherche devraient préalablement informer les utilisateurs de manière transparente des traitements de données réalisés lors de l'utilisation de leurs services.

2. En vue de la sensibilité des traces que laissent les utilisateurs lors de l'utilisation d'un moteur de recherche, les fournisseurs de moteurs de recherche devraient offrir leurs services de manière à respecter la vie privée. Plus spécifiquement, ils n'enregistreront pas d'information sur la requête qui puisse être reliée aux utilisateurs de moteur de recherche, ni d'information sur les utilisateurs eux-mêmes. A la fin d'une session de recherche, aucune donnée pouvant être liée à un utilisateur

individuel ne devrait être stockée, à moins que l'utilisateur ait consenti de manière explicite et informée au fait que ses données stockées seront stockées aux fins de se voir offrir un service (par exemple pour l'utilisation dans des recherches futures).

3. Quoiqu'il advienne, le principe de minimisation de données est fondamental. Une telle pratique serait également avantageuse pour les fournisseurs de moteurs de recherche en simplifiant les modalités de réponse aux demandes émanant de tiers quant à la fourniture d'informations relative à un utilisateur spécifique[5].

[5] Pour les besoins de cette résolution, „tiers" signifiera la personne physique ou morale, l'autorité publique, le service ou tout organisme autre que la personne concernée, le responsable de traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont habilitées à traiter les données.

4.7 Recommandation au Tribunal pénal fédéral: «Rapport sur les griefs relatifs au faible nombre d'actes d'accusation prononcés par le Ministère public de la Confédération»

Voir paragraphe 4.7 de la partie en langue allemande.

4.8 Recommandation adressée à l'Office fédéral des transports: «Rapports annuels des exploitants de téléphériques»

Voir paragraphe 4.8 de la partie en langue allemande.

4.9 Recommandation adressée au Département fédéral des affaires étrangères: «Détection précoce des risques en matière de visas»

Voir paragraphe 4.9 de la partie en langue allemande.