13ème Rapport d'activités 2005/2006

Préposé fédéral à la protection des données

Rapport d'activités 2005/2006 du Préposé fédéral à la protection des données

Le Préposé fédéral à la protection des données est tenu de fournir périodiquement au Conseil fédéral un rapport sur son activité (article 30 de la loi fédérale sur la protection des données). Le présent rapport couvre la période du 1er avril 2005 au 31 mars 2006.

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

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.013.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Le point culminant de l'année 2005 a été incontestablement la 27ème Conférence internationale des commissaires à la protection des données et à la protection de la vie privée que nous avons organisée à Montreux, du 14 au 16 septembre. Plus de 350 participants venus du monde entier ont pris part à une rencontre très enrichissante qui a suscité un grand intérêt tant sur le plan national qu'international. La Conférence avait pour thème: «Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités»; elle a trouvé son apogée dans la déclaration finale, qui a été l'occasion de renforcer l'universalité des principes de la protection des données. Nous sommes persuadés que cette déclaration de Montreux donnera une impulsion majeure à la diffusion et au développement, à l'échelle internationale, de la protection de la personnalité. Je tiens à remercier celles et ceux qui ont contribué au succès de cette rencontre, tout particulièrement la Chancelière de la Confédération, dont l'importante participation financière accordée sur son budget a tout simplement permis à la 27ème Conférence de voir le jour. La Conférence a adopté deux résolutions importantes. La première traite de l'utilisation des données biométriques dans les passeports, les cartes d'identité et les documents de voyage, la seconde concerne l'utilisation de données personnelles dans la communication politique (pour plus de détails, se reporter au compte rendu détaillé figurant au chiffre 9.2.1).

Parmi les grands thèmes que nous avons traités cette année, citons notamment les applications diverses de la biométrie (passeport biométrique, contrôle d'accès aux installations de loisirs, contrôle à l'enregistrement et à l'embarquement dans les aéroports, contrôle à l'occasion de manifestations sportives, etc.), l'utilisation de drones (pour la surveillance des frontières entre autres), la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, la carte de santé, ainsi que d'autres thèmes touchant à la santé.

Si nous jetons un regard rétrospectif sur l'année écoulée, il apparaît clairement que nous avons effectivement renforcé nos tâches de surveillance comme le prévoyait la réorganisation du service. En témoignent les nombreux projets menés à terme, notamment le contrôle de l'utilisation de la biométrie à l'enregistrement et à l'embarquement à l'aéroport de Zurich, les programmes de fidélisation de la clientèle Cumulus et Supercard, le contrôle dans les domaines de la recherche médicale et des biobanques, des cartes de crédit, etc. Nous avons constaté avec satisfaction que les responsables des domaines dans lesquels nous avons exercé notre mission de surveillance ont toujours accompagné nos travaux de manière très positive. Ils les ont considérés comme

une circonstance opportune en vue d'une meilleure protection de la personnalité et ont su mettre en application nos recommandations, en reconnaissant qu'une protection des données fiable et bien gérée constitue le meilleur programme de fidélisation des clients. L'évolution extrêmement rapide de la technologie amène chaque jour son lot de nouveaux risques potentiels et va exiger de notre part dans le futur une activité de surveillance accrue. Mais, en même temps, nous devons souligner que pour donner des résultats crédibles, les projets de surveillance menés avec sérieux demandent vraiment beaucoup de temps et requièrent des ressources considérables. C'est pour cette raison qu'il nous est d'ores et déjà impossible d'exercer nos tâches de surveillance dans tous les domaines qu'il conviendrait de prendre en considération. Ceci d'autant plus que nos autres tâches, notamment de conseil aux particuliers et à l'administration, ne cessent de se multiplier. Déjà aujourd'hui nous ne sommes pas en mesure de traiter toutes les demandes qui nous parviennent. Notre activité de surveillance demeure donc très limitée et nous nous voyons toujours contraints de réduire notre activité de conseil. A cela s'ajoute le fait que l'évolution de la technique élargit inéluctablement l'éventail des domaines touchant à la protection des données. L'administration recourt de plus en plus à e-government, à e-health, à l'utilisation des numéros personnels d'identification, pour ne citer que quelques exemples. Ces projets représentent une lourde charge de travail. De ce fait, nous nous voyons toujours davantage obligés de repousser ou même de laisser totalement de côté des projets urgents en matière de conseil et de surveillance. Cela dit, si nous désirons accomplir notre mission dans ces deux domaines de manière à peu près crédible, nous ne devons plus accepter aucune réduction quant au nombre des projets à concrétiser annuellement.

Pour cette raison, je ne peux que m'inquiéter des mesures d'économie qui ne cessent de mettre sous pression l'effectif de notre autorité de protection des données, déjà très serré et extrêmement modeste en comparaison internationale.

De nouvelles tâches importantes viennent sans cesse s'ajouter à nos activités. La loi fédérale sur le principe de la transparence dans l'administration, qui entrera en vigueur prochainement, nous impose - en cas de litige - la tenue de procédures de médiation entre les citoyens et l'administration fédérale. Une autre de nos tâches est d'informer et de conseiller les personnes ou entreprises concernées par l'application de la loi. En même temps, il est prévisible que les Accords bilatéraux, en particulier l'approbation des accords de Schengen/Dublin, nous imposeront aussi de nouvelles tâches de surveillance. En ce qui concerne ces accords, qui ont fait l'objet de bien des controverses justement en raison de la menace potentielle qu'ils représentent pour la sphère privée des citoyennes et des citoyens, nous avons toujours souligné que nous

ne pouvons examiner la conformité au droit de la protection des données que si nos ressources nous le permettent. D'après l'état actuel du débat, cela ne semble pas encore être le cas: les postes supplémentaires dont nous aurions besoin du fait de la loi sur la transparence et des nouvelles tâches de surveillance découlant de Schengen/Dublin ne nous ont pas été encore accordés. Qui plus est, nos effectifs diminueront d'ici la fin 2006 et passeront de 19, 6 postes à 19.

La période 2006-2007 sera donc une année décisive pour la protection des données en Suisse: pourrons-nous continuer à assurer une protection des données crédible? Je m'engagerai personnellement à ce qu'elle le demeure et ne cesserai d'informer le public de l'impact que des programmes d'économie sans différenciation pourraient avoir sur la protection des données.

Hanspeter Thür

Répertoire des abréviations

ASSM	Académie suisse des sciences médicales
CFPD	Commission fédérale de la protection des données
CIP-E	Commission des institutions politiques du Conseil des Etats
CP	Code pénal
CSSS-N	Commission de la sécurité sociale et de la santé publique du Conseil national
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFJP	Département fédéral de justice et police
DFI	Département fédéral de l'intérieur
FOSC	Feuille officielle suisse du commerce
ISA	Système d'information relatif aux documents d'identité
LAGH	Loi fédérale sur l'analyse génétique humaine
LAMal	Loi fédérale sur l'assurance-maladie
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LN	Loi fédérale sur l'acquisition et la perte de la nationalité (Loi sur la nationalité)
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi fédérale sur la protection des données
METAS	Office fédéral de métrologie et d'accréditation
OACI	Organisation de l'aviation civile internationale
OAMAS	Ordonnance concernant l'appréciation médicale de l'aptitude au service et de l'aptitude à faire service

OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFP	Office fédéral de la police (actuellement fedpol)
OFRF	Office fédéral chargé du droit du registre foncier et du droit foncier
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFSPO	Office fédéral du sport
PFPD	Préposé fédéral à la protection des données
RFID	Radio Frequency Identification
SAP	Service d'analyse et de prévention
SAS	Service suisse d'accréditation
SIS	Système d'information de Schengen

1 Droits fondamentaux

1.1 Modernisation de la protection des données

1.1.1 Procédure de certification dans le cadre du projet de révision de la loi fédérale sur la protection des données

Une procédure de certification volontaire en matière de protection de données est prévue dans le cadre du projet de révision de la LPD. En ce qui concerne la certification d'organisations, un référentiel type en deux parties sera soumis à des entreprises certificatrices pour appréciation. La première partie porte sur les exigences que doit remplir un système de gestion de protection des données, tandis que la seconde se concentre sur une grille de vérification de conformité, soit sur les exigences concrètes de protection des données dérivées de la LPD.

Dans le cadre de la révision de la LPD, nous avons poursuivi notre collaboration avec l'OFJ et le SAS/METAS (cf. notre 12ème rapport d'activités 2004/2005, chiffre 1.1.2), dans le but de définir les exigences minimales relatives à l'obtention d'une certification en matière de protection des données pour une organisation ou une procédure de traitement des données. Nous avons ainsi cherché à définir plus précisément un référentiel type, devant permettre - d'une part – de vérifier l'existence et le fonctionnement concret d'un système de gestion de protection des données (SGPD) dans l'organisation auditée, et - d'autre part - de contrôler que le niveau de protection des données au moment de l'audit répond aux exigences de la législation en vigueur. Pour ce faire, il nous a paru judicieux de séparer le référentiel type en deux parties distinctes: la première portant sur le SGPD, la seconde sur la concrétisation des exigences de protection des données.

Pour définir les exigences d'un SGPD, nous nous sommes inspirés de celles formulées dans le récent standard ISO/IEC 27001:2005 (anciennement BS 7799-2:2002) pour les systèmes de gestion de la sécurité de l'information (SGSI). A cet égard, l'art. 7 al. 1 LPD (Sécurité des données) dispose que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Nous rappellerons que le standard d'audit ISO/IEC 27001:2005 se base complètement sur le standard ISO/IEC 17799:2005, qui comprend 15 chapitres et 134 contrôles au total, parmi lesquels le 15.1.4 porte spécifiquement sur la conformité des traitements de données personnelles. C'est ce dernier contrôle que nous avons concrétisé à la lumière de la LPD et qui forme la seconde partie du référentiel type, appelée «grille de vérification de conformité».

L'hypothèse de travail est la suivante: avec pour conditions un niveau de protection des données reconnu conforme au moment de l'audit et l'apport d'un SGPD, grâce auquel le niveau de protection des données doit en principe se maintenir (voire s'améliorer), les exigences de protection des données devraient être respectées durablement. Une certification de protection des données peut alors être délivrée pour une période de quelques années, durant laquelle des audits intermédiaires sont prévus et au terme de laquelle un nouvel audit complet aura lieu.

Notre objectif est maintenant de soumettre notre projet de référentiel type aux entreprises de certification ayant l'expérience des normes ISO 900x et/ou ISO 17799, dans le but d'en assurer son intégrité et son applicabilité.

1.1.2 Transfert de données personnelles par les compagnies aériennes aux autorités américaines et canadiennes

La communication de données personnelles sur les passagers aux autorités américaines par les compagnies aériennes soumises à la législation suisse sur la protection des données est réglée par un accord conclu entre la Suisse et le Etats-Unis. Celui-ci a été avalisé par le Conseil fédéral le 4 mars 2005. Dans cet accord, les autorités américaines fournissent les mêmes garanties que celles accordées à l'Union européenne. Sous l'angle de la protection des données, cet accord peut être jugé comme acceptable. Un accord similaire a été conclu le 16 mars 2006 avec le Canada.

Dans notre 11ème rapport d'activités 2003/2004, nous avons défendu la position que la communication de données personnelles par les compagnies aériennes aux autorités américaines basée sur un accord entre la Suisse et les Etats-Unis était la meilleure solution au regard des exigences de la législation sur la protection des données. En novembre 2004, un tel accord a été conclu entre la Suisse et les Etats-Unis. Cet accord, similaire à celui conclu entre l'Union Européenne et les Etats-Unis, a été avalisé par le Conseil fédéral le 4 mars 2005. Il peut être jugé comme acceptable sous l'angle de la protection des données. La liste des données à transmettre est moins longue que celle initialement requise. Les données sensibles, par exemple les données sur l'état de santé ou celles permettant de déterminer la religion d'un passager, ne sont pas communiquées aux autorités américaines. Les données ne peuvent être traitées qu'à des fins de lutte contre le terrorisme et la criminalité internationale. La durée de conservation des données a été fixée à 42 mois au lieu des 50 ans demandés par les Etats-Unis. En plus de l'information fournie par les compagnies aériennes, les autorités

américaines renseignent les passagers sur l'autorité responsable de la collecte de données personnelles, la finalité de la collecte, les traitements effectués ainsi que sur les procédures relatives au droit d'accès et au droit de rectification. Dans ce cadre, le Préposé fédéral à la protection des données peut agir pour le compte d'une personne concernée. Les autorités américaines effectueront cette année avec les autorités suisses une révision commune de la mise en œuvre de l'accord.

Un accord similaire a été conclu avec le Canada le 16 mars 2006.

Le texte de l'accord avec les Etats-Unis est accessible sur le site de l'Office fédéral de l'aviation civile:

http://www.aviation.admin.ch/imperia/md/content/bazl/aktuell/medienmitteilungen/95.pdf.

Le texte de l'accord avec le Canada est également accessible sur le même site à l'adresse suivante:

http://www.aviation.admin.ch/imperia/md/content/bazl/aktuell/medienmitteilungen/123.pdf

1.2 Autres thèmes

1.2.1 Harmonisation des registres, identificateur de personnes et recensement de la population

En vue du recensement de la population de 2010, on a cherché à harmoniser les registres de personnes. Il était prévu d'introduire un identificateur de personnes pour faire le lien entre les différents registres existants. Plusieurs projets ont été élaborés à cette fin. Le dernier projet en date prévoit d'harmoniser les registres en utilisant le numéro AVS comme référence commune dans tous les registres. Nous préconisons cependant de considérer également d'autres modèles pour le recensement de la population à partir de registres.

En mars 2004, le Conseil fédéral a pris connaissance des résultats de la procédure de consultation pour la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes et a demandé au Département fédéral de l'intérieur (DFI) d'élaborer le message. Au cours de la procédure de consultation, la question de l'introduction d'identificateurs de personnes coordonnés a également été soulevée.

L'Office fédéral de la statistique (OFS) a élaboré plusieurs projets relatifs à l'identificateur de personnes, projets qui ont été soumis à plusieurs consultations. Après le rejet de l'identificateur fédéral de personnes harmonisé (EPID), il était prévu de remplacer ce dernier par un système comportant six identificateurs sectoriels de personnes (SPIN). Nous avons demandé que les registres soient attribués aux différents secteurs et que ces secteurs soient définis de manière concrète, ce qui n'a jamais été fait. Sur la base des résultats de la procédure de consultation relatif au SPIN, le Conseil fédéral a, en octobre 2004, mandaté clairement le DFI de limiter l'introduction de l'identificateur de personnes à la population (IFPP) en utilisant le numéro STAR, l'identifiant du registre informatisé d'état civil INFOSTAR. En novembre 2004 ont eu lieu les consultations des offices concernant le projet de message pour une loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes (LHR) ainsi que le projet de message pour une loi fédérale sur l'identificateur de personnes du secteur «population» (BPIN).

Le 10 juin 2005, le Conseil fédéral a chargé le DFI d'élaborer un message pour une loi fédérale sur l'harmonisation des registres et de le soumettre aussi rapidement que possible aux Chambres fédérales. Il a également décidé que le nouveau numéro AVS devrait être introduit comme référence commune dans certains registres de personnes au niveau fédéral, cantonal et communal.

Il est prévu de remplacer l'actuel numéro AVS par ce nouveau numéro à partir de 2008. Ce numéro (appelé également numéro d'assuré ou numéro d'assurance sociale) devrait faire office d'identificateur de personnes pour la statistique ainsi que pour l'administration. En ce qui concerne le NIP, cela représente un pas en direction d'un identificateur de personnes commun, avec tous les risques qui y sont associés (cf. à ce sujet notre 12ème rapport d'activités 2004/2005, chiffre 1.2.1; 10ème rapport d'activités 2002/2003, chiffre 1.2.1). Le nouveau numéro AVS a été prévu comme numéro d'identification pour le domaine de l'assurance sociale et à notre avis son utilisation doit donc être restreinte à ce domaine.

Nous sommes d'avis que la Suisse devrait étudier d'autres modèles, tels que le modèle autrichien, qui représente une solution moderne et tournée vers l'avenir; cette solution présenterait aussi des avantages pour une future application de cyberadministration. Le modèle autrichien est basé sur des numéros spécifiques à des domaines ainsi que sur une série de transformations cryptographiques. Il faudrait à tout prix éviter de mélanger les domaines de la statistique et de l'administration, les exigences de ces deux domaines étant différentes aussi bien du point de vue de la quantité que de la qualité des données. L'utilisation de numéros spécifiques à chaque domaine réduit également le risque que les données soient mises en relation. L'utilisation du

numéro AVS n'est actuellement pas limitée par la loi, ce qui a pour conséquence que l'usage de ce numéro a, au cours du temps, été étendu bien au-delà du domaine de l'AVS et même jusque dans le secteur commercial et privé. Il est impératif que l'usage du numéro d'assuré comme identificateur général de personnes soit clairement réglé et que les mesures techniques et organisationnelles qui s'y rapportent soient définies. L'absence de délimitation du cercle des usagers ainsi que l'absence de définition du but poursuivi dans la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) ouvrent tout grand la porte aux utilisations les plus diverses de ce numéro (détournement de finalité).

Il serait préférable d'adapter le modèle autrichien aux exigences suisses. Ceci nous permettrait d'avoir une solution conforme aux exigences de la protection des données et qui a l'avantage d'avoir déjà été mise en œuvre et d'avoir fait ses preuves.

1.2.2. La protection de la sphère privée dans le cadre d'une procédure de naturalisation

Dans le cadre d'une procédure de naturalisation par décision de l'assemblée communale ou par scrutin populaire, la publication d'informations personnelles sur le candidat à la naturalisation est disproportionnée du point de vue de la protection de la sphère privée. Une solution conforme à la LPD serait d'attribuer la compétence d'examiner les dossiers de candidature à un cercle restreint de personnes soumis au devoir du secret, par exemple une commission spéciale.

Au début de l'année 2005, nous avons été invités à prendre position sur l'avant-projet de modification de la loi sur la nationalité (LN), élaboré par la Commission des institutions politiques du Conseil des Etats (CIP-E). Ce projet concrétisait une initiative parlementaire lancée suite à deux arrêts du Tribunal fédéral qui avait notamment jugé la procédure de naturalisation par scrutin populaire inconstitutionnelle. Le projet de la CIP-E avait pour but de concilier la tradition de naturalisation par décision de l'assemblée communale ou par votation populaire et les exigences d'un Etat de droit; selon la proposition de la CIP-E, les cantons auraient expressément la compétence pour fixer la procédure de naturalisation au niveau du canton et des communes, mais devraient prévoir une obligation de motivation de la décision et un droit de recours au niveau d'une dernière instance cantonale.

Nous avons exprimé nos doutes quant à la compatibilité entre la naturalisation par scrutin populaire et les droits fondamentaux. Toutefois, nous avons essentiellement apprécié la proposition du CIP-E sous l'angle de la protection de la sphère privée. De

ce point de vue, l'attribution de la compétence aux cantons pour fixer la procédure en matière de naturalisation ne nous a pas paru, en soi, problématique. Néanmoins, le projet de la CIP-E attribuait aux cantons la compétence de déterminer les données pouvant être rendues publiques; à cet égard, il était toutefois précisé que seules les données personnelles «indispensables» portant sur la nationalité et la durée de résidence ainsi que les informations générales relatives au respect de l'ordre juridique et à l'intégration pouvaient être rendues publiques.

Nous avons estimé que la publication de toutes ces données personnelles à l'attention de l'ensemble des citoyens était disproportionnée.

La publication de données personnelles du candidat à la naturalisation constitue une atteinte à la sphère privée, qui n'est licite que si elle est prévue par la loi, justifiée par un intérêt prépondérant et si elle est proportionnée. En l'espèce, il existe un intérêt public à ce que l'organe de décision dispose d'informations relativement détaillées sur le candidat à la naturalisation afin d'être en mesure d'apprécier si les conditions pour la naturalisation sont remplies et de se prononcer ainsi sur l'octroi de la nationalité. Dans ce contexte, des données sensibles telles que les activités politiques ou même religieuses peuvent être pertinentes pour estimer si le candidat à la naturalisation est bien intégré; de même, le fait de savoir si cette personne a déjà été condamnée paraît indispensable pour vérifier si elle respecte l'ordre juridique suisse.

Toutefois, la *publication* – à l'attention de l'ensemble de la population - des informations relatives à la nationalité, la durée de résidence et les informations relatives à l'ordre juridique et à l'intégration est disproportionnée: les conditions matérielles à l'octroi de la naturalisation (durée de résidence, intégration, respect de l'ordre juridique suisse, etc.) sont prévues par la Loi fédérale sur la nationalité et sont notamment examinées par une autorité fédérale (Office fédéral des migrations) lors de l'octroi de l'autorisation fédérale de naturalisation. Même si les cantons ont la possibilité d'examiner ces conditions dans le cadre de leur procédure, il existe des mesures plus respectueuses de la protection de la sphère privée des personnes concernées que la publication de l'ensemble de ces données.

Il serait par exemple envisageable de prévoir, dans le cadre de la procédure cantonale, une commission spéciale compétente pour traiter les dossiers des candidats à la naturalisation; cette autorité, impliquant un cercle restreint de personnes soumis au devoir du secret, aurait accès à toutes les données personnelles nécessaires à l'examen des conditions de naturalisation. Une telle solution pourrait être considérée comme proportionnée et conforme à la LPD.

1.2.3 Contrat-type pour l'externalisation du traitement de données à l'étranger

Lorsqu'une entreprise suisse envisage de confier le traitement de ses données à l'étranger (*outsourcing*), nous lui recommandons de conclure un contrat pour régler le transfert de données hors des frontières. Nous avons élaboré un contrat-type en collaboration avec David Rosenthal de l'étude d'avocats zurichoise Homburger. Ce contrat sert à garantir une protection adéquate des données personnelles au sens de la LPD. Il a été conçu spécialement pour les entreprises suisses et repose sur le droit suisse, bien qu'il reflète pour une bonne part la teneur de contrats-types similaires élaborés dans le cadre de l'Union européenne et du *Safe Harbour Agreement*. La conclusion d'un tel contrat s'impose en particulier lorsque les données doivent être transférées dans des pays qui ne connaissent pas de dispositions de protection des données semblables à celles de la Suisse.

Le contrat-type est disponible sur notre site www.edsb.ch, et peut également être trouvé dans l'annexe 11.1.

2 Protection des données – Questions d'ordre général

2.1 Protection et sécurité des données

2.1.1 Expériences pratiques avec le règlement de traitement

Au début du contrôle que nous effectuons dans le cadre de notre activité de surveillance, nous exigeons généralement du maître de fichier le règlement de traitement, afin de pouvoir nous faire une première idée du système à contrôler. Nous constatons régulièrement que les règlements de traitement ne correspondent pas encore aux prescriptions.

Ayant reçu de nombreuses demandes de la part de responsables de la protection des données à propos de ce qui devait figurer exactement dans un règlement de traitement, nous avons créé une table des matières devant servir de modèle et décrivant en détail les points à documenter du point de vue de la protection des données. Cette table des matières peut être téléchargée sur notre site web http://www.edsb.ch/f.

Nous devons cependant constater aujourd'hui encore que les règlements ne sont pas élaborés à temps, ou seulement de manière incomplète, par les services responsables. Ceci surprend dans la mesure où de nombreux éléments contenus dans le règlement de traitement sont indispensables pour la planification et la réalisation correcte et transparente d'un système, ainsi que pour son exploitation. Il résulte de l'absence de documentation un manque de transparence et de contrôlabilité des systèmes. Ceci rend plus difficile notamment le respect de la protection des données.

Dans le cadre de notre activité de surveillance, nous nous faisons généralement une première vue d'ensemble en examinant le règlement de traitement. Pour les maîtres de fichiers ou les responsables de la protection des données, il est important que le règlement contienne les critères que nous avons indiqués. Bien entendu, il est également possible que certains points devant normalement être mentionnés ne soient pas significatifs pour certains systèmes. Ceci doit alors être expressément mentionné dans le règlement. Pour l'élaboration du règlement de traitement, il faut s'en tenir au principe de documenter autant que nécessaire, mais aussi peu que possible. Pour des informations plus détaillées, il convient de renvoyer aux différents documents. L'important est la transparence et la facilité de compréhension du règlement.

Nous allons continuer à l'avenir de rendre les maîtres de fichiers attentifs à leur devoir d'élaborer un règlement de traitement.

2.1.2 Traces électroniques au sein de l'administration fédérale

Les activités effectuées sur ordinateur laissent des traces électroniques, dont une partie contiennent des données personnelles. La collecte et le traitement de ces dernières sont soumis à la LPD. Selon la loi, l'administration fédérale a besoin d'une base légale pour pouvoir traiter ces données.

Aujourd'hui, la plupart des tâches professionnelles et privées sont effectuées à l'aide d'un ordinateur. Toutes ces activités laissent des traces électroniques, à partir desquelles il est théoriquement possible de reconstruire les actions de l'utilisateur (qui, quoi et quand). Le potentiel d'intrusion dans la sphère privée est important. Si les activités en question sont effectuées sur la place de travail, c'est très souvent l'employeur qui, à l'aide des traces électroniques, a la possibilité d'accéder à des données personnelles.

Selon la LPD, un organe fédéral a besoin d'une base légale pour pouvoir traiter de telles données personnelles. Nous avons cherché à connaître le genre de traces électroniques laissées dans le cadre de nos propres activités et récoltées par les services informatiques (cf. notre 12ème Rapport d'activités 2004/2005, chiffre 2.1.2.). L'Office fédéral de l'informatique et de la télécommunication (OFIT) nous a remis une liste exhaustive des informations récoltées, qui comprennent non seulement le genre de traces traitées, mais aussi les temps de conservation et l'existence d'éventuelles copies de sauvegarde. Ces travaux nous ont permis de rendre l'OFIT attentif à la nécessité d'élaborer une base légale pour régler le traitement de telles données. Dans son avis de droit sur cette problématique, l'office fédéral de la justice est arrivé aux mêmes conclusions.

2.2 Autres thèmes

2.2.1 Engagement des drones de reconnaissance au profit du Corps des gardes-frontière

Le Corps des gardes-frontière voudrait faire surveiller les frontières nationales à l'aide de drones de reconnaissance de l'armée. Or ces vols de reconnaissance ne se limitent pas à surveiller les entrées illégales en Suisse: une multitude de citoyens n'ayant rien à se reprocher tomberaient également dans l'objectif des caméras-vidéos des drones. L'utilisation des drones requiert une base légale expresse et suffisante dans le droit fédéral.

A la demande du Corps des gardes-frontière, des drones de reconnaissance de l'armée (petits avions sans pilote) seront utilisés dès janvier 2006 pour surveiller le territoire suisse dans les zones frontières, cela dans le cadre de l'engagement du service d'appui afin de renforcer le Corps des gardes-frontière et d'assurer la sécurité aux frontières (engagement de l'armée LITHOS). Ces drones permettront de lutter contre la contrebande, contre la criminalité transfrontière et la migration illégale. Equipés de caméras et d'appareils de vision nocturne, les drones surveillent l'espace frontalier. Selon les déclarations du Corps des gardes-frontière, cet espace s'étend à de larges portions des cantons frontaliers. De grandes agglomérations comme Bâle et Genève en font également partie.

Indépendamment de ce cas, l'armée de l'air a reçu un nombre accru de demandes émanant des autorités civiles (états-majors de crise cantonaux, forces de police, etc.). Celles-ci désirent utiliser les drones notamment pour la surveillance des manifestations, la gestion du trafic routier (embouteillage au Gothard), voire même pour la recherche de criminels.

Nous avons mené, avec les offices fédéraux concernés (armée de l'air et Corps des gardes-frontière), de longues discussions sur l'engagement des drones et la conformité aux principes de la protection des données. Nous n'avons par ailleurs jamais remis en cause le fait que les drones puissent contribuer efficacement à repérer les entrées illégales sur le territoire national. Cela étant, nous ne sommes pas parvenus à un accord avec les deux services fédéraux mentionnés sur les points ci-dessous:

- Les prises de vue aériennes effectuées à l'aide des drones doivent-elles être qualifiées de données personnelles, au sens de la LPD?
- Les dispositions de la législation douanière invoquées par le Corps des gardes-frontière constituent-elles une base légale suffisante, au sens de la LPD?

Les prises de vue aériennes sont des données personnelles

L'armée de l'air et le Corps des gardes-frontière sont d'avis que l'utilisation des drones n'implique pas du tout un traitement de données personnelles.

Conformément à la LPD, les données personnelles sont toutes les informations qui se rapportent à une personne identifiée ou identifiable. L'utilisation des drones a pour but de déterminer le lieu de séjour de personnes et de surveiller leurs mouvements. Une personne peut être identifiée sans difficulté par les forces d'intervention mobiles du Corps des gardes-frontière sur place ou à l'aide d'autres moyens. Si cette identification donne suite à des poursuites ou à des sanctions administratives ou pénales, nous sommes même en présence de données sensibles. Si les drones sont mis en œuvre sur une longue durée afin de déterminer le comportement d'une personne, il s'agit alors d'un profil de la personnalité au sens de la LPD.

Du point de vue du droit de la protection des données, peu importe que les drones utilisés actuellement ne permettent pas d'obtenir des images à haute résolution (par exemple, il est impossible de lire les numéros de plaque de véhicules). Ce n'est probablement qu'une question de temps avant que les caméras soient équipées de zooms suffisamment performants.

Par conséquent, les prises de vue aériennes faites dans le cadre de vols ayant pour but la surveillance et donc en définitive l'identification de personnes, constituent des données personnelles au sens de la LPD. Les organes fédéraux ne peuvent traiter des données personnelles sensibles ou des profils de la personnalité que si une loi fédérale les y autorise expressément. La loi sur l'armée autorise l'utilisation de drones uniquement dans le cadre de la tâche principale de l'armée. Toute utilisation de drones de reconnaissance dans le cadre d'une assistance en faveur d'autres autorités nécessite une base légale propre et explicite dans une loi fédérale. Celle-ci doit au moins établir le but et la portée de l'utilisation des drones, définir les responsabilités et les destinataires des données. Elle déterminera également la marche à suivre en cas de découvertes fortuites, sans rapport avec le franchissement de la frontière.

La législation douanière n'est pas une base légale suffisante

Le Corps des gardes-frontière estime que la législation douanière légitime d'ores et déjà suffisamment l'utilisation de drones. Conformément à la loi fédérale sur les douanes, l'Administration des douanes peut avoir recours à des appareils de prise de vues et de relevé afin de déceler le franchissement illégal de la frontière ou des dangers pour la sécurité à la frontière. Les détails sont réglés par l'ordonnance sur la surveillance de la frontière verte au moyen d'appareils vidéo. Selon cette ordonnance, il est

possible d'utiliser des appareils vidéo pour garantir la sécurité de la ligne des douanes et la perception des droits ainsi que pour surveiller le franchissement de la frontière.

Sur la base des travaux préparatoires et des textes relatifs à l'utilisation d'appareils vidéo à la frontière (ordonnance du 26 octobre 1994 sur la surveillance de la frontière verte à l'aide d'appareils vidéos; messages relatifs à la loi fédérale du 1er octobre 1925 sur les douanes et à la nouvelle loi fédérale du 18 mars 2005 sur les douanes; Bulletin officiel du Parlement), nous avons établi que le législateur n'avait réglementé que l'utilisation au sol d'appareils automatiques de prise de vues et de relevé. Les textes des messages accompagnant les actes législatifs sur les douanes ne mentionnent ni les enregistrements ni les relevés faits à partir d'un drone, pas plus que le législateur ne s'est exprimé, au cours des délibérations parlementaires, sur une éventuelle intervention de l'armée de l'air.

Par ailleurs, il convient de souligner que les prises de vue aériennes impliquent une qualité particulière de traitement des données par rapport aux enregistrements effectués à l'aide de caméras vidéos installées au sol. Les caméras vidéos installées au sol permettent une surveillance très limitée dans l'espace; les prises de vue aériennes permettent par contre de surveiller les personnes au sol sans point d'attache géographique, sans limitation à un endroit, ni limitation dans le temps. En outre, les drones peuvent fonctionner en restant largement inaperçus. Les prises de vue aériennes constituent donc un plus grand risque d'atteinte aux droits de la personnalité que les prises de vues effectuées à partir d'une caméra installée au sol. En effet, ce sont non seulement les personnes visées (soit les migrants illégaux) mais aussi une grande partie de la population qui tombent dans l'objectif des caméras. Cette partie de la population doit prendre en compte une surveillance potentielle, même si elle ne menace en aucun cas la sécurité des frontières ou ne désire pas du tout immigrer illégalement. Ne serait-ce que pour cette raison, le Parlement doit se prononcer sur le caractère légal de l'atteinte aux libertés fondamentales de la population et donner une base légale suffisante à l'utilisation des drones.

Proposition de compromis

Nous ne sommes en principe pas contre l'utilisation de drones au profit du Corps des gardes-frontière, mais nous visons la conformité avec la LPD et le respect de la protection de la personnalité, en particulier des personnes n'ayant rien à se reprocher. Nous avons donc proposé une solution de transition aux offices fédéraux concernés. Cette proposition repose sur l'art. 17a du projet de révision de loi sur la protection des données: selon cette disposition, le Conseil fédéral peut autoriser le traitement

automatisé de données personnelles sensibles ou de profils de la personnalité pour un projet pilote même si les bases légales formelles nécessaires manquent encore et doivent encore être créées par le Parlement.

Alors qu'un accord sur ce point nous semblait acquis et que les offices fédéraux concernés avaient élaboré en commun une proposition dans ce sens au Conseil fédéral, le Département fédéral des finances nous a informés de manière inattendue qu'il ne soumettrait pas la proposition au Conseil fédéral. Il a estimé que la législation douanière constituait déjà une base légale suffisante pour l'utilisation des drones et nous a informés que dès janvier 2006, le Corps des gardes-frontière allait demander à l'armée de l'air de commencer les vols de reconnaissance à l'aide de drones, sans demander l'accord du Conseil fédéral.

2.2.2 Révision partielle de la loi sur l'armée et l'administration militaire

Le DDPS a entrepris une révision de la loi sur l'armée et l'administration militaire. Cette révision vise en premier lieu la création de bases légales appropriées pour le traitement de données personnelles. Sous l'angle du droit de la protection des données, l'avant-projet peut encore être amélioré.

Nous avons déjà traité des problèmes de protection des données en rapport avec la mise en oeuvre d'Armée XXI (voir notre 12ème rapport d'activités 2004/2005, chiffre 2.2.1, ainsi que notre 11ème rapport d'activités 2003/2004, chiffre 2.2.1). Nous avons à chaque reprise critiqué le fait qu'il manque, dans la loi sur l'armée, les bases légales requises par la LPD pour le traitement de données personnelles sensibles ou de profils de la personnalité et que le contenu des ordonnances soumises au Conseil fédéral n'était souvent pas suffisamment détaillé.

Selon les informations de la Chancellerie fédérale, à l'occasion de l'adoption de la révision totale de l'ordonnance concernant l'appréciation médicale de l'aptitude au service et de l'aptitude à faire service (OAMAS), le Conseil fédéral a enjoint le DDPS à entreprendre rapidement une révision partielle de la loi sur l'armée pour ce qui concerne la protection des données. Dans le cadre de ces travaux actuellement en cours, le DDPS nous a soumis un premier avant-projet de révision des dispositions de protection des données figurant dans la loi sur l'armée et nous a demandé de nous prononcer à son sujet.

Nous avons à cette occasion constaté que de nombreuses dispositions de l'avant-projet ne satisfaisaient pas aux exigences de la LPD. Ainsi, on ne peut parler de base légale suffisante lorsqu'une disposition accorde globalement à tous les offices fédéraux la possibilité de traiter des données personnelles. Pas plus que nous ne pouvons considérer comme suffisante la formulation selon laquelle «un office fédéral peut traiter toutes les données qui lui sont indispensables pour l'accomplissement de ses tâches».

Les bases légales du traitement de données doivent être suffisamment concrétisées du point de vue du contenu. Il convient à cet égard de respecter les exigences minimales suivantes:

- définition du but du traitement,
- détermination, dans les grandes lignes, de l'étendue du traitement des données,
- désignation expresse des personnes participant au traitement des données (personnes traitant les données, destinataires éventuels des données),
- mention des catégories de données traitées (dans la mesure où des données sensibles ou des profils de la personnalité sont concernés).

Ces exigences minimales découlent du principe de la légalité et du principe de transparence. La formulation doit être suffisamment claire pour que le citoyen puisse adapter son comportement et mesurer les conséquences qu'aura pour lui le traitement des données. Le DDPS a donné l'assurance que nos remarques seront prises en compte lors du remaniement de l'avant-projet.

2.2.3 Révision de l'ordonnance relative au registre foncier

Le projet de révision de l'ordonnance prévoyait de faciliter la communication à des particuliers de données extraites du registre foncier; il aurait été permis de transférer des données sur des supports de données électroniques et par procédure d'appel. Pour des motifs relevant de la protection des données, le transfert de données par CD-ROM a été abandonné; s'agissant de la procédure d'appel, des lettres-types obligatoires destinées aux préposés cantonaux au registre foncier seront mises au point.

Bien que la LPD ne soit pas applicable aux registres publics de droit privé (catégorie dont fait partie le registre foncier), l'Office fédéral chargé du droit du registre foncier et du droit foncier (OFRF) nous a soumis, dans le cadre de la consultation des offices, les modifications apportées à l'ordonnance sur le registre foncier, en nous priant de nous prononcer à leur sujet.

La législation spéciale consacrée aux différents registres réglemente aussi explicitement la manière dont le traitement des données personnelles doit avoir lieu. Afin d'éviter que ces réglementations ne se heurtent à la LPD, le législateur a exclu ces registres du domaine d'application de la LPD.

Cela ne signifie pas pour autant que les principes de la protection des données ne doivent pas être respectés dans la législation sur la tenue des registres. Du reste, une obligation de tenir compte et de respecter les principes de la protection des données découle également du Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE n° 108) concernant les autorités de contrôle et les flux transfrontières de données.

La modification de l'ordonnance avait notamment pour objectif de faciliter la communication de données personnelles figurant dans les registres fonciers:

D'une part, les offices du registre foncier auraient dû avoir la possibilité de mettre à disposition de certaines catégories d'utilisateurs les données du registre foncier, par transfert de données (par ex. sur CD-ROM). Nous nous sommes prononcés contre une telle possibilité. En effet, dans un tel cas, les responsables n'auraient plus la maîtrise sur les données traitées. Le destinataire aurait toute latitude pour traiter les données reçues sans qu'on ne puisse rien y faire (par ex. il pourrait transmettre les données à d'autres personnes, ou encore les modifier). En qualité de responsable initial des données, l'Office du registre foncier perdrait tout contrôle sur les données remises. Sensible à nos préoccupations, l'OFRF a accepté de supprimer cette disposition.

D'autre part, les banques, les caisses de pension et les assurances auraient dû avoir un accès direct, par procédure d'appel, à toutes les données du registre foncier dont ils auraient eu besoin pour remplir leurs tâches dans le domaine des affaires hypothécaires. Nous avons émis des doutes quant à la nécessité d'ouvrir les registres fonciers à ces particuliers; nous y voyons une violation du principe de proportionnalité. A notre avis, il existe des moyens et des procédures qui portent une atteinte moins importante à la personnalité des individus concernés et qui respectent ainsi le principe de proportionnalité (par ex. extrait traditionnel du registre foncier).

L'OFRF a maintenu sa proposition pour des raisons d'efficacité. Nous avons néanmoins pu nous entendre sur le fait que les cantons soient obligés de conclure avec les utilisateurs des conventions relatives à l'utilisation ultérieure des données obtenues. Ces conventions sont conformes aux modèles obligatoires de l'OFRF. Elles doivent au moins régler le type et le mode d'accès, son contrôle, la finalité du traitement des données obtenues, la protection contre l'accès non autorisé par des tiers, les restrictions quant à leur transmission à des tiers ainsi que les conséquences du traitement abusif des données.

2.2.4 Publication sur Internet de données extraites du registre du commerce

Un particulier ne peut traiter des données extraites du registre du commerce que s'il peut produire un motif justificatif. L'analyse de crédit ne peut être considérée comme motif justificatif que si le tiers peut justifier d'un intérêt à obtenir ces données.

Selon ses propres déclarations, une entreprise reprend les données du registre du commerce publiées dans la Feuille officielle suisse du commerce FOSC et les publie sur son site web. Son objectif est de permettre d'accéder à toutes les entreprises, personnes et publications enregistrées dans le registre du commerce depuis 1996. Dès lors, lorsque l'on introduit un prénom et un nom dans un moteur de recherche Internet, on obtient comme résultat un lien sur le portail Internet de l'entreprise en question. Le site de celle-ci mentionne toutes les inscriptions relatives à la personne recherchée figurant dans la FOSC et il est également possible de demander des informations économiques sur son entreprise.

De nombreuses personnes se sont plaintes de ce genre de publication. L'entreprise défend le point de vue selon lequel elle met les données de la FOSC telles quelles à la disposition des internautes et que le contexte spécifique du registre officiel est ainsi sauvegardé. En outre, elle invoque pour cette forme de traitement des données le motif justificatif de l'analyse de crédit mentionné dans la LPD.

Le simple fait que le registre du commerce soit public ne signifie pas qu'une entreprise puisse reprendre son contenu et traiter les données en question sans tenir compte de la LPD. Le but premier et principal de la publication des données du registre du commerce est la sécurité du droit dans les affaires et la protection de la bonne foi (fonction de publicité). Le Code des obligations a donné cette tâche et la responsabilité du registre du commerce aux autorités compétentes et non à des particuliers. L'entreprise en question ne peut donc pas se fonder sur ce motif justificatif pour traiter des données. Quelle que soit la forme de réutilisation de données personnelles, elle a besoin d'un motif justificatif conforme à la loi sur la protection des données.

Le motif justificatif invoqué par l'entreprise (l'analyse de crédit) permet de traiter des informations concernant la solvabilité d'une personne et, dans certaines conditions, de les communiquer à des tiers. Selon la loi, on ne peut communiquer à des tiers que les données dont il a besoin pour conclure ou exécuter un contrat avec la personne concernée. Cela implique que le tiers puisse se prévaloir d'un intérêt s'il veut obtenir ces données (par ex. négociations contractuelles en cours avec la personne concernée). La simple curiosité d'un internaute ne suffit pas. La personne traitant les données est chargée de vérifier la présence de cet intérêt. La question se pose de savoir comment procéder à cette vérification dans le cas d'une publication accessible sans restriction sur Internet.

A la suite de notre intervention, l'entreprise mentionnée nous a informés qu'elle était prête à publier ces données uniquement si la personne intéressée pouvait démontrer ou rendre vraisemblable de manière appropriée un intérêt à leur obtention. Nous allons suivre l'évolution de cette affaire et vérifier les mesures prises.

2.2.5 Système biométrique de contrôle d'accès à un centre sportif

La vérification biométrique d'identité est en pleine expansion pour le contrôle d'accès à des installations publiques. Pour répondre aux préoccupations des abonnés concernés, nous avons décidé de procéder à un contrôle du nouveau système biométrique de contrôle d'accès mis en place dans un centre sportif privé. Nous analysons à présent les données récoltées, en les évaluant à l'aune des principes fondamentaux de protection des données.

Sollicités par plusieurs citoyens préoccupés par l'introduction d'un système biométrique de contrôle d'accès à un centre sportif privé, nous avons décidé de procéder à un contrôle sur place. Comme à l'accoutumée, nous avons annoncé notre visite à la direction de l'établissement et nous avons préalablement demandé un éclaircissement quant au concept envisagé et posé quelques questions de base. Après examen des réponses fournies, nous nous sommes rendus sur les lieux pour constater et vérifier les traitements de données effectués, afin de compléter notre éclaircissement des faits. En l'état actuel, une empreinte digitale est saisie au moment de la conclusion d'un abonnement annuel et conservée dans le système central, sous la forme d'un gabarit biométrique. Lors de chaque visite à la piscine, l'abonné introduit son empreinte digitale – dont le gabarit extrait doit correspondre à la référence mémorisée dans le système central - afin de libérer le portail d'accès. Un des buts avoués de ce nouveau type d'authentification biométrique est de prévenir les abus (notamment par transmission de carte entre personnes proches). La carte ne contient aucune donnée personnelle, mais uniquement un numéro personnel d'identification lisible par radiofréquence (RFID). En cas d'oubli, l'abonné peut se présenter au guichet et attester de son identité, afin d'accéder aux installations. Nous avons également porté notre attention sur le traçage des entrées des clients, sur les délais de conservation des différentes données et sur les multiples statistiques issues de ce nouveau système de gestion. Après dépouillement et analyse des informations qui nous ont été fournies, nous adresserons à la direction de l'établissement un rapport définitif comprenant des appréciations, des propositions d'amélioration ou, selon les résultats de notre examen, une recommandation au sens de l'art. 29 al. 3 LPD.

2.2.6 Contrôle de l'utilisation de la biométrie à l'enregistrement et à l'embarquement à l'aéroport de Zurich-Kloten

Le projet pilote Secure Check a été mené à l'aéroport de Zurich-Kloten de décembre 2004 à mi-avril 2005. Ce projet visait à améliorer le contrôle de sécurité des données des passagers et des documents de voyage avant le départ grâce à l'utilisation de données biométriques et à raccourcir les délais d'attente des passagers aux points de contrôle. Suite à notre contrôle de l'utilisation de la biométrie à l'enregistrement et à l'embarquement, nous avons donné une appréciation essentiellement positive de l'usage fait des données biométriques. Quelques réflexions fondamentales s'imposent toutefois quant à l'utilisation de la biométrie à l'aéroport de Zurich-Kloten.

En décembre 2004, Checkport Suisse SA a lancé en collaboration avec Swissport Suisse SA et SWISS International Airlines le projet pilote Secure Check à l'aéroport de Zurich-Kloten. Dans le cadre de notre fonction d'autorité de surveillance en matière de protection des données dans le secteur privé, nous avons suivi la phase de test du projet pilote et en avons contrôlé les processus du point de vue de la protection des données. Le contrôle a porté en priorité sur le relevé et le traitement des données biométriques. Comme le projet pilote faisait appel pour la première fois à une nouvelle technologie (le procédé biométrique), qui impliquait le traitement de données personnelles sensibles, il était indispensable que l'examen des faits et le contrôle de la protection des données aient lieu avant la mise en œuvre du projet pilote.

Nous avons rencontré deux fois les acteurs concernés de Swissport, Checkport et SWISS à Zurich-Kloten pour un examen des faits sur place. Dans une première phase du projet pilote, deux empreintes digitales des passagers ont été scannées et converties en gabarits (templates) pour permettre leur authentification à la porte d'embarquement. Dans une seconde phase, les deux empreintes digitales ont été remplacées par deux images faciales (templates). Lors de ces deux visites, il est apparu que la fiabilité de la reconnaissance variait selon les caractéristiques biométriques utilisées; nous avons constaté que l'authentification était plus fiable dans le cas des images faciales. Tant les gabarits des empreintes digitales que ceux des images faciales ont été enregistrés sur une carte à puce (smart card) que les passagers ont gardée sur eux jusqu'à la porte d'embarquement. Dans le contexte du projet pilote Secure Check, les données biométriques n'ont jamais été stockées de manière centralisée.

Sur la base du contrôle effectué en vertu de l'art. 29 LPD, nous avons donné une appréciation essentiellement positive de l'usage fait des données biométriques. Les mesures prises dans le cadre du projet pilote en vue d'une mise en œuvre définitive vont dans la bonne direction du point de vue de la protection des données. Dans notre rapport final, nous avons toutefois fait quelques observations fondamentales quant à l'utilisation de la biométrie, que la direction du projet devrait prendre en compte et traduire dans les faits lors de la mise en œuvre définitive du projet Secure Check.

En particulier les points suivants devraient être examinés de très près:

- Il faudrait accroître la transparence du traitement des données en ce sens que les personnes concernées devraient être informées clairement de toutes les catégories de données traitées (identité, vol, biométrie, statistiques, etc.) et cela, depuis la saisie des données jusqu'à leur destruction. Il convient de s'assurer tout particulièrement que les données ont bien été effacées physiquement (et non seulement logiquement), en temps voulu (soit le plus tôt possible) et intégralement (fichiers temporaires compris).
- Une telle saisie de données biométriques - qui constitue une première - peut susciter de nouvelles convoitises de la part de tiers tels que la police aéroportuaire ou les autorités d'immigration étrangères. Nous avons donc demandé à la direction du projet de prendre conscience de ces convoitises lors de la mise en œuvre définitive de Secure Check et, notamment, de ne pas transmettre de données biométriques à des tiers (tels que des autorités) sans motif justificatif (par ex. une base légale; cf. art. 13 al. 1 LPD).
- Toute modification du projet Secure Check allant dans le sens d'un stockage centralisé des données biométriques ou d'un stockage de données brutes nécessiterait, sous l'angle de la protection des données, une appréciation différenciée qui n'est pas couverte par le présent rapport. De même, il conviendrait de revoir et de redéfinir la finalité du projet si les données biométriques saisies devaient être transmises à des autorités étrangères au cours d'une phase ultérieure.

Etant donné qu'une authentification à l'aide de caractéristiques biométriques ne saurait être fiable à 100 %, nous avons par ailleurs recommandé de recourir, lors de la mise en œuvre définitive du projet Secure Check, à un système d'authentification multimodale (par combinaison avec d'autres caractéristiques personnelles telles qu'un numéro personnel d'identification). En outre, pour les personnes dont les caractéristiques biométriques font défaut ou ne sont que difficilement lisibles, il est important de planifier et de mettre à disposition une alternative permettant de les authentifier de manière sûre et fiable.

Le rapport intégral en langue allemande peut être consulté sur notre site web www.edsb.ch.

2.2.7 Vente de billets personnalisés pour les manifestations sportives de grande envergure

Ces dernières années, les organisateurs de manifestations sportives ont procédé de plus en plus souvent à des ventes de billets personnalisés. En parallèle, les travaux de législation avancent dans le domaine de la lutte contre la violence lors de manifestations sportives de masse (hooliganisme). Nous accompagnons d'une part ces travaux de législation dans le domaine de la sécurité publique. D'autre part, en vue de l'EURO 08, nous effectuons des recherches auprès des organes responsables de la vente des billets, dans la mesure où leur siège se trouve en Suisse.

En nous référant aux travaux de législation intitulés «Sécurité et lutte contre la violence lors de manifestations de grande envergure», nous ne mentionnerons ici brièvement que les deux principaux éléments prévus. Il s'agit en premier lieu d'une banque de données sur les personnes connues comme hooligans, avec les règles correspondantes sur la saisie et la suppression des inscriptions. Le deuxième élément important de la législation prévoit des mesures telles que l'interdiction de stade et l'interdiction de pénétrer dans un périmètre déterminé. Pour de plus amples informations sur les travaux de législation, nous renvoyons au chiffre 3.1.2 du présent rapport d'activités.

La vente de billets personnalisés a été pour la première fois appliquée à grande échelle à l'occasion des championnats d'Europe de football au Portugal (EURO 04). Cette manière de procéder a essentiellement été motivée par l'argument «sécurité»: ce n'est qu'en vérifiant l'identité de tous les visiteurs qu'il serait possible de déterminer si des hooligans se trouvent parmi eux. Cependant, l'effet secondaire de ce procédé est de générer une importante collection de données personnelles qui peut s'avérer extrêmement intéressante notamment pour le marketing. Pour cette raison, lors de

l'EURO 04, les organisateurs portugais avaient exigé des bureaux de vente des billets de proposer à leurs clients une possibilité de s'opposer à l'utilisation de leurs données à des fins publicitaires. Cependant, dans de nombreux pays, cette exigence n'a pas été appliquée par les points de vente de billets. En Allemagne particulièrement, cette lacune a suscité une certaine attention de la part de la presse.

Nous partons du principe que l'EURO 08 qui se déroulera en Autriche et en Suisse donnera également lieu à une vente de billets personnalisés. Il s'agit donc de faire en sorte que des erreurs telle que celle mentionnée ci-dessus ne se répètent pas. Pour cette raison, nous avons pris contact avec l'Office fédéral du sport (OFSPO), avec l'UEFA et avec l'Association suisse de football (ASF), ainsi qu'avec d'autres partenaires tels que l'Office fédéral de la police (OFP) et les autorités cantonales.

En ce qui concerne la Coupe du monde 06, nous avons pris contact avec la FIFA en janvier 2005 et nous avons mené des recherches jusqu'en novembre 2005. Celles-ci ont mis en évidence que la FIFA avait omis d'imposer à l'organe organisant les jeux en Allemagne des prescriptions en matière de protection des données. Une deuxième constatation insatisfaisante est que, dans le point de vente des billets en ligne, la FIFA se procure auprès des acquéreurs de billets un «consentement» préventif pour l'utilisation et la transmission de leurs coordonnées à des fins non déterminées. Et finalement, en troisième lieu, selon ses propres déclarations, la FIFA ne détient pas de banque de données des interdictions de stades, contrairement à ses directives de sécurité publiées sur Internet (http://www.fifa.com/documents/static/regulations/FIFA_Safety_Guidelines_F.pdf).

Compte tenu de l'état avancé des travaux pour la Coupe du Monde 06, nous n'avons pas poursuivi notre intervention. Nous avons toutefois communiqué à la FIFA que sa responsabilité était maintenue et que nous nous en tenions à sa déclaration selon laquelle elle ne détenait pas de banque de données des interdictions de stade. En ce qui concerne l'avenir, notre déclaration envers la FIFA mentionnait que celle-ci devait entreprendre des démarches concrètes pour améliorer la situation et nous en tenir informés. La FIFA a pris connaissance de ces recommandations pour optimiser la situation du point de vue de la protection des données. Elle nous a également confirmé qu'elle nous tiendrait au courant de toute évolution de la situation.

3 Justice/Police/Sécurité

3.1 Affaires de police

3.1.1 Révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure

Dans le cadre de la consultation des offices, nous avons été invités à prendre position sur deux projets consécutifs de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI II). Dans notre prise de position relative au premier projet, nous avons estimé que les nouvelles mesures prévues ne respectaient pas les droits fondamentaux, notamment du fait qu'elles constituaient des atteintes disproportionnées à la sphère privée. Dans notre prise de position relative au second projet de révision, nous avons - en dépit des changements apportés - maintenu nos critiques et estimé que le nouveau projet de révision n'était pas conforme aux principes de protection des données.

1er projet de révision

Au mois de juillet 2005, nous avons été invités à prendre position sur un premier projet de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Il était notamment prévu d'étendre le champ d'application de la loi à la criminalité organisée et d'attribuer à l'office fédéral de la police des compétences plus étendues. En particulier, le projet de révision prévoyait la possibilité pour le Service d'analyse et de prévention (SAP) de disposer de «moyens de recherche spéciale d'informations» (tels que la surveillance de la correspondance par poste et télécommunication, l'observation dans des lieux privés ou au moyen d'appareils techniques de surveillance, la perquisition secrète d'un système informatique) en dehors de toute procédure pénale. Ces mesures, analogues aux moyens existant actuellement dans le cadre d'une procédure pénale pendante, seraient – à la différence des mesures de contrainte prononcées par les autorités de poursuite pénale - ordonnées à l'encontre de personnes sur lesquelles ne pèse aucun soupçon concret de comportement punissable. Dans le cadre de ce premier projet, il était prévu que certaines mesures soient soumises à une commission spécialisée indépendante pour autorisation, tandis que d'autres mesures étaient soumises à la seule appréciation de l'office.

Nous nous sommes d'emblée montrés très critiques à l'égard de ce premier projet de loi. Les mesures projetées constituent des atteintes graves aux droits fondamentaux des personnes concernées, en particulier à la protection de la sphère privée. Par ailleurs, aucune protection juridique n'était prévue. L'information ultérieure des personnes concernées n'était pas davantage réglée. Nous avons estimé que ce projet n'était pas compatible avec les droits fondamentaux.

Nous avons constaté que les moyens actuellement à disposition des autorités compétentes (soit du SAP, mais également des autorités de police et de justice pénale) n'avaient pas été évalués. De même, d'autres moyens permettant de lutter contre le terrorisme n'avaient pas été examinés (p. ex. amélioration de la coopération entre les autorités compétentes dans le domaine de la lutte contre le terrorisme, ou encore développement du droit pénal et de la procédure pénale). Ni la nécessité, ni la proportionnalité des mesures proposées n'avait été démontrée. En particulier, nous avons fait remarquer que la gravité de l'atteinte à la sphère privée n'avait pas été comparée avec le bénéfice correspondant pour la sécurité. Si la sécurité intérieure et extérieure de la Suisse représente un intérêt public indéniable, il ne peut d'emblée justifier des mesures aussi attentatoires à la sphère privée. Chacune des mesures doit être évaluée sous l'angle de la proportionnalité. Le but légitime de la lutte contre le terrorisme ne saurait priver d'emblée les personnes concernées de leurs libertés et de leurs droits fondamentaux.

Nous avons relevé qu'un certain nombre de dispositions du Code pénal permettent actuellement aux autorités de poursuite pénale d'intervenir très tôt dans la commission de l'acte punissable, soit dans une phase préventive, avant même la commission de l'acte proprement dit. Selon la législation actuellement en vigueur, les autorités compétentes peuvent ordonner les mesures de contrainte qui s'imposent (écoute téléphonique, perquisition, etc.) dès l'apparition d'un soupçon concret de comportement punissable: Ainsi, les actes préparatoires à certaines infractions capitales (meurtre, assassinat, lésions corporelles graves, etc.) sont répréhensibles pour eux-mêmes et une personne est punissable déjà au stade de la planification de l'infraction (art. 260bis CP). De même, le simple fait d'appartenir à une organisation criminelle est également punissable (art. 260ter CP). Une autre disposition du Code pénal prévoit la répression du financement du terrorisme (art. 260^{quinquies} CP). En outre, il existe déjà de nombreuses possibilités, dans le cadre d'une procédure pénale, de maintenir le secret à l'égard de la personne concernée.

A la suite de cette première consultation des offices, le chef du Département de justice et police a, en automne 2005, renvoyé le projet à ses auteurs et les a chargés d'élaborer un nouveau texte.

2ème projet de révision

Au début de l'année 2006, nous avons été invités à prendre position sur le second projet de révision. Celui-ci se distancie sur plusieurs points du premier texte soumis en consultation au mois de juillet 2005; en particulier, nous avons retenu que l'on avait renoncé à inclure la criminalité organisée du champ d'application de la LMSI et que la recherche spéciale d'informations était désormais limitée à certains domaines particuliers. De plus, les droits fondamentaux des particuliers ont davantage été pris en compte, en ce sens que le nouveau projet prévoit notamment l'obligation d'informer ultérieurement les personnes observées (avec des exceptions possibles) et une possibilité de recours.

Selon la procédure prévue par le second projet de révision (procédure d'autorisation), toutes les mesures de recherche spéciale devraient être ordonnées par le chef du département, impliquant ainsi une responsabilité politique; contrairement au premier projet de révision, plus aucune distinction ne serait faite entre les différentes mesures. Ces dernières seraient préalablement soumises à l'autorisation d'une «commission indépendante de contrôle» composée de trois membres nommés par le Conseil fédéral. L'avis positif de l'autorité de contrôle constituerait ainsi une condition sine qua non pour permettre au SAP de procéder aux mesures spéciales. Néanmoins, en cas d'urgence, le SAP aurait la possibilité d'appliquer les mesures prévues sans attendre le feu vert de la commission de contrôle et du chef du département (procédure d'urgence); dans un tel cas, une autorisation ultérieure de ladite commission serait nécessaire.

En dépit des changements apportés, nous avons maintenu notre position critique quant à la nécessité d'une révision de la LMSI, en particulier de la nécessité et de la proportionnalité des nouvelles mesures projetées. En outre, nous avons exprimé nos doutes quant à l'application de l'obligation de communiquer et quant à l'effectivité du droit de recours, de même qu'à l'efficacité des contrôles devant être effectués par ladite Commission de contrôle indépendante.

Nous avons considéré que la nécessité des mesures n'avait pas été démontrée de manière convaincante; en particulier, nous avons constaté qu'aucun exemple n'avait été cité pouvant démontrer ou au moins rendre vraisemblable que les moyens actuels ne seraient pas suffisants pour lutter contre le terrorisme et prévenir des menaces contre la sécurité intérieure.

Le projet de révision «LMSI II» donne au SAP la possibilité d'ordonner des mesures de contrainte analogues à celles existantes dans le cadre d'une procédure pénale pendante; toutefois ces mesures ne seraient pas soumises aux mêmes conditions d'application. En effet, le SAP aurait la possibilité d'intervenir et de mettre en œuvre des moyens de contrainte à un stade bien plus avancé que ne le permettrait la procédure pénale, à savoir lorsqu'il n'y a que «des suppositions et de vagues indices» et non lorsqu'il existe un soupçon concret de comportement punissable. Nous avons soutenu qu'une recherche spéciale d'informations au moyen de mesures contraignantes ne saurait se faire que sur la base d'un soupçon concret de commission d'un acte punissable ou d'un acte préparatoire. En admettant l'usage de moyens de contrainte sans qu'il n'existe un soupçon concret d'infraction pénale, on s'écarte des fondements mêmes d'un Etat de droit.

Dans la mesure où le projet de révision devait être adopté, en dépit de nos critiques, nous avons demandé que l'application de la loi soit au moins limitée dans le temps, et qu'une évaluation de l'efficacité des nouvelles mesures prévues ait lieu à l'issue d'une période déterminée.

Au-delà de ces remarques fondamentales concernant la nécessité de nouvelles mesures, nous avons notamment pris position sur les points suivants:

Autorité de contrôle indépendante. Nous avons soutenu que l'autorité de contrôle indépendante devrait être une autorité judiciaire, et qu'elle devrait, en tout état de cause, être élue par le Parlement et composée de magistrats de l'ordre judiciaire. Indépendamment de la composition de l'autorité de contrôle, nous soutenons toutefois que cette dernière n'est pas à même de juger sur la base de vagues indices.

Protection absolue des sources. Il est prévu d'étendre la protection des sources, de façon absolue, à toutes les informations provenant de sources internes, et non plus seulement pour les informations en provenance de l'étranger. Nous nous opposons à une telle modification, car nous estimons que les informateurs de mauvaise foi et ceux qui se rendent coupables d'une infraction n'ont pas un droit à être absolument protégés. Leur responsabilité pénale ou civile devrait être engagée en cas de délit ou de crime grave ou en cas d'information volontairement fausse. En outre, la législation en vigueur prévoit déjà que la transmission de données personnelles n'est pas autorisée lorsqu'elle est contraire à des intérêts publics ou privés prépondérants

Procédure d'urgence. Dans le cas où des données ont été collectées dans le cadre de la procédure d'urgence mais que l'autorité de contrôle indépendante par la suite refuse son approbation, se pose le problème de l'utilisation des données dans l'intervalle: Dans un tel cas de figure, on ne peut garantir que les données communiquées entre temps à des tiers seront détruites. Il est en particulier douteux que les services étrangers détruiront ces informations. Nous avons proposé que lorsqu'une telle situation se présente, l'autorité de contrôle indépendante statue sans délai sur la question spécifique de la communication à des tiers, selon une procédure simplifiée.

Obligation de communiquer - Information ultérieure. La jurisprudence du Tribunal fédéral et de la Cour européenne des droits de l'homme exige que la personne ayant fait l'objet d'une observation secrète en soit en principe informée ultérieurement. Cette condition est une conséquence de la garantie du respect de la vie privée et du secret de la correspondance et doit également permettre à la personne concernée de faire valoir son droit à un recours effectif.

Le présent projet de révision prévoit que la communication ultérieure soit d'emblée restreinte. Or nous estimons que les éléments communiqués ne permettent pas à la personne de faire valoir ses droits, notamment son droit à un recours effectif. Nous sommes d'avis que d'éventuelles restrictions (notamment pour des raisons d'intérêt public) doivent être examinées au cas par cas. Par ailleurs, un renseignement fondé sur l'art. 18 al. 6 LMSI suite au dépôt du droit d'accès indirect interviendrait trop tard et ne permettrait pas à la personne de faire valoir ses droits à temps.

Droit d'accès indirect. Finalement, nous remettons en question le droit d'accès indirect à l'occasion de la révision de la LMSI; il convient de réévaluer cette pratique sur la base de l'expérience acquise à cet égard depuis l'entrée en vigueur de la LMSI. L'article 18 LMSI prévoit que le PFPD vérifie la licéité du traitement des données dans le fichier ISIS, et la personne concernée ne reçoit en principe aucune information sur les éventuelles données enregistrées.

3.1.2 Protection des données et lutte contre le hooliganisme

Dans le cadre de la consultation des offices, nous avons pris position sur le projet de modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (loi fédérale sur les mesures contre la propagande incitant à la violence et contre la violence lors de manifestations sportives, LMSI I). Cette loi prévoit notamment l'introduction d'une «banque de données sur le hooliganisme». Bien que certaines de nos remarques aient été retenues dans le projet de loi, quelques différends et questions ouvertes subsistent. Par ailleurs, suite à notre prise de position et en réponse à une demande, nous avons soutenu que l'utilisation d'un système de reconnaissance faciale biométrique n'est pas couverte par le présent projet de loi.

Le projet de loi LMSI I, sur lequel nous nous étions déjà exprimés une première fois en 2002 (cf. notre 10ème rapport d'activités 2002/2003, chiffre 3.1.2) prévoit notamment l'introduction d'un système d'information dans lequel sont enregistrées des données de personnes ayant fait preuve d'un comportement violent lors de manifestations sportives (banque de données sur le hooliganisme).

Une partie de nos remarques ont été retenues dans le projet de loi, mais certaines questions subsistent. Ainsi, nous sommes d'avis que le message devrait exprimer avec plus de précision quelles sont les conditions exactes qui caractérisent un cas de «violences lors de manifestations sportives». En effet, de tels cas doivent pouvoir être distingués d'autres cas moins graves de «violence spontanée», qui relèvent de la compétence de la police cantonale. Le projet de loi prévoit notamment qu'une mesure prononcée (notamment l'interdiction de stade et la limitation de voyager à l'étranger) doit pouvoir être enregistrée dans le système d'information si elle est nécessaire au maintien de la sécurité des personnes ou des manifestations sportives et s'il peut être rendu vraisemblable qu'elle est motivée. A notre avis, cette disposition est formulée trop vaguement et doit être supprimée. Ceci d'autant plus que le projet de loi prévoit déjà d'enregistrer dans le système d'information les mesures prononcées ou confirmées par une autorité judiciaire, ou les dénonciations transmises à l'autorité compétente. Par ailleurs, il ne ressort ni du projet de loi, ni du message, quel rôle et quelles compétences la nouvelle loi accordera au bureau central du hooliganisme rattaché à la police municipale de Zurich. Il s'agit aussi de savoir comment la répartition des compétences entre ce dernier et l'Office fédéral de la police sera réglée. Il n'y a pas de réponse non plus sur la manière dont sera réglée la répartition des tâches des organisateurs en leur qualité de personnes privées d'une part et en tant que responsables d'une tâche publique d'autre part.

A la suite des consultations des offices, on nous a demandé si l'utilisation d'un système de reconnaissance faciale biométrique était couverte par l'actuel projet de loi. Nous avons relevé que le recours à un système de reconnaissance faciale biométrique devait être expressément réglé dans une loi au sens formel (par exemple le projet en cours). Le projet dans sa forme actuelle ou une simple réglementation par ordonnance ne seraient donc pas suffisants. Par ailleurs, la vidéosurveillance ne devrait en aucun cas être assimilée à la reconnaissance faciale biométrique, car cette dernière constitue une atteinte bien plus importante à la personnalité des personnes concernées. Avant de créer une base légale appropriée, il faudrait en outre vérifier le respect des principes fondamentaux de la protection des données (en particulier le principe de finalité et de proportionnalité). Si la reconnaissance faciale biométrique devait également être utilisée par des personnes privées (comme les organisateurs de manifestations sportives ou d'autres tiers), ceux-ci devraient non seulement respecter les principes fondamentaux de la protection des données, mais également disposer d'un motif justificatif pour le traitement des données (consentement, intérêt public ou privé prépondérant, base légale).

3.1.3 Droit d'accès indirect

Dans notre dernier rapport d'activités, nous avons rapporté que, suite à une décision de la Commission fédérale de la protection des données (CFPD), nous avons adapté notre pratique en ce qui concerne la vérification des demandes d'accès indirect. Nous avons maintenant eu l'occasion de présenter notre nouvelle pratique à l'occasion d'une séance avec la CFPD et l'Office fédéral de la police.

Sur la base d'une décision de la Commission fédérale de la protection des données (CFPD), nous avons adapté notre procédure relative au droit d'accès indirect (cf. notre 12ème rapport d'activités 2004/2005, chiffre 3.1.3). Comme déjà mentionné dans notre dernier rapport d'activités, certains points de la décision de la CFPD nécessitaient d'être tirés au clair. A cette fin, une première séance a eu lieu le 26 novembre 2004 avec la CFPD, l'Office fédéral de la police (OFP) et nous-mêmes. La discussion a porté sur notre nouvelle pratique, ainsi que sur nos vérifications des demandes d'accès indirectes en général. La CFPD a posé diverses questions et, tant l'OFP que nous-mêmes avons pu rendre compte en détail des expériences acquises, des difficultés rencontrées et des points positifs. A la suite de cette séance, la CFPD a déclaré qu'elle approuvait en principe la nouvelle pratique adoptée par le PFPD pour la vérification des demandes d'accès indirect. Toutefois, comme certains points étaient encore en suspens, la CFPD a décidé de poursuivre ultérieurement la discussion.

Dans le cadre de différents cas, la CFPD nous a aussi priés de prendre position sur l'interprétation de diverses dispositions de l'art. 18 de la loi fédérale sur les mesures visant au maintien de la sûreté intérieure (LMSI), ainsi que de l'art. 14 de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC). Elle nous a en même temps invités à en débattre à l'occasion d'une séance qui s'est déroulée le 15 février 2006.

3.1.4 Contrôles en matière d'information ultérieure des personnes concernées

L'Office fédéral de la police (OFP) nous a soumis un concept pour le système d'information JANUS relatif à la mise en œuvre de l'information ultérieure des personnes concernées dans le domaine de la police, prévue par la loi. L'OFP n'a vu aucune raison de développer un concept identique pour le système d'information GEWA, car dans ce cas il ne collectait pas lui-même les données. Nous avons analysé le concept JANUS et avons proposé quelques modifications. En même temps, nous avons demandé à l'OFP d'appliquer un concept analogue pour GEWA. L'OFP n'a pas accepté les propositions de modifications et a maintenu sa position en ce qui concerne GEWA. Nous avons porté l'affaire devant le DFJP pour décision.

Dans notre dernier rapport d'activités, nous avons rendu compte de notre examen des faits et des recommandations correspondantes sur l'information ultérieure des personnes concernées dans le domaine de la police (cf. notre 12ème rapport d'activités 2004/2005, chiffre 3.1.1). L'Office fédéral de la police (OFP) devait, en relation avec la mise en œuvre de l'art. 14 al. 1 de la loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC), élaborer un concept et nous le soumettre.

Malgré plusieurs échanges de correspondance, une documentation détaillée et une séance, il n'était toujours pas clair comment l'OFP voulait précisément appliquer la disposition mentionnée. En outre, dans les différents courriers de l'OFP, nous n'avons pas pu déceler de concept proprement dit indiquant les critères selon lesquels les personnes concernées pourraient être informées. Pour cette raison, nous avons accordé à l'OFP un délai supplémentaire pour nous communiquer si les personnes concernées seraient effectivement informées au sens de l'art. 14 al. 1 LOC et, dans l'affirmative, pour nous soumettre des concepts succincts pour les systèmes d'information en question (JANUS et GEWA). L'OFP nous a alors fait parvenir un concept relatif à JANUS. En ce qui concerne GEWA, l'OFP a maintenu qu'il n'y avait aucune raison de développer un processus d'exécution pour l'application de l'art. 14 al.1 LOC, car GEWA

n'impliquait pas de collecte initiale de données, c'est-à-dire que la collecte de données pour GEWA serait effectuée par d'autres autorités que l'OFP. Nous avons ensuite analysé le concept relatif à JANUS. Nous avons surtout été frappés du fait que, pour JANUS aussi, l'OFP opère une distinction entre les données personnelles qu'il collecte lui-même et celles qu'il reçoit de la part de tiers, les personnes concernées au sens de l'art. 14 al. 1 LOC n'étant jamais informées lorsque les données sont acquises par un tiers. A ce sujet, nous avons soutenu que l'art. 14 al. 1 LOC ne mentionne pas que l'information ultérieure ne doit avoir lieu que si les données sont collectées directement. C'est pourquoi il y a lieu de vérifier dans chaque cas si l'information ultérieure de la personne concernée peut avoir lieu ou non, peu importe que les données aient été collectées directement ou par des tiers. En même temps, nous avons demandé à l'OFP s'il était prêt à adapter son concept en fonction de nos propositions de modification et d'appliquer le même concept par analogie à GEWA. L'OFP n'a pas accepté nos propositions de modification, mais a suggéré de mettre en œuvre son concept pour JANUS dans une phase pilote et de discuter avec nous du concept après évaluation de du projet pilote.

Après avoir analysé la réponse de l'OFP, nous avons constaté que nos recommandations n'ont pas été suivies. Nous avons porté l'affaire devant le DFJP pour décision.

3.1.5 Introduction de données biométriques dans le nouveau passeport suisse

Dès septembre 2006, des passeports biométriques seront établis en Suisse dans le cadre d'un projet pilote devant durer cinq ans. Durant la phase de planification, nous avons pris contact avec les services responsables de l'Office fédéral de la police afin de nous assurer du respect des principes de la protection des données. En parallèle, nous nous sommes prononcés, dans le cadre de la procédure de consultation, sur la révision de la loi fédérale et de l'ordonnance fédérale sur les documents d'identité. Un point nous a semblé disproportionné dans la révision de la loi, à savoir l'enregistrement des données biométriques de la personne titulaire du passeport dans une banque de données centrale.

En septembre 2004, suivant l'évolution observée au niveau international dans le domaine des documents de voyage, le Conseil fédéral a mandaté le DFJP de procéder à une révision de la loi sur les documents d'identité et de l'ordonnance sur les documents d'identité. A la demande des Etats-Unis et sur la recommandation de l'Organisation de l'aviation civile internationale (OACI), le passeport suisse sera désormais muni d'une puce contenant des données biométriques. L'enregistrement de données biométriques (l'image du visage, puis dans un second temps les empreintes digitales) permettra une identification claire du titulaire du passeport, rendant ainsi très difficile l'abus en matière de documents d'identité. L'image du visage et ultérieurement les empreintes digitales, seront relevées dans des centres de saisie biométrique. Les données seront enregistrées sur la puce et dans le système d'information relatif aux documents d'identité (ISA). Les premiers passeports biométriques seront établis dès septembre 2006 dans le cadre d'une phase pilote de cinq ans; pour cette phase pilote, seule la saisie de l'image du visage est prévue. Ce projet est fondé sur la révision de l'ordonnance sur les documents d'identité. L'introduction définitive des passeports biométriques nécessitera une révision de la loi sur les documents d'identité.

Les données biométriques sont des données personnelles sensibles au sens de l'art. 3, let. c, ch. 2 LPD, car elles permettent par exemple de tirer des conclusions sur l'appartenance raciale ou sur des maladies. La présente révision et en particulier le projet pilote devront absolument faire l'objet d'un examen quant à la finalité et la proportionnalité de l'enregistrement de données biométriques dans le passeport suisse, notamment quant à son caractère approprié et nécessaire. A cet égard, il convient de relever que la Suisse est liée à certaines directives émises par des organismes internationaux (OACI, UE) quant à l'introduction des passeports biométriques.

Au cours de la procédure de consultation, nous avons souligné que le projet pilote ne reposait sur aucune base légale suffisante. En effet, le traitement de données personnelles sensibles requiert une base légale formelle (art. 17 al. 2 LPD). L'ordonnance révisée sur les documents d'identité ne remplit pas cette condition. Par ailleurs, nous estimons que l'enregistrement centralisé de données biométriques brutes dans la banque de données ISA est disproportionné; le but du passeport biométrique - l'authentification de son titulaire au moment où il présente son document d'identité - peut aussi être atteint en comparant les données de référence (image digitalisée du visage, empreintes digitales) avec la personne présente. Le fait que selon l'ordonnance révisée, les données de l'ISA ne puissent pas être utilisées à des fins de recherche n'enlève rien au caractère disproportionné de l'enregistrement centralisé. Par ailleurs, il est prévu que la lecture de la puce aux frontières internationales sera réglée par des conventions bilatérales. Nous avons demandé la création de garanties contractuelles suffisantes pour que les données biométriques ne soient pas utilisées de manière abusive. Ceci s'impose d'autant plus avec les pays qui ne disposent pas d'une législation sur la protection des données équivalente à la législation suisse. Nous estimons en outre prématuré de permettre aussi à des entreprises de transport, qui doivent contrôler l'identité de leurs passagers, d'accéder aux données biométriques figurant dans le passeport. Les possibilités actuelles de vérification du titulaire du billet de transport nous semblent suffisantes. Enfin, nous avons demandé, en ce qui concerne l'utilisation de puces RFID, que des mesures adaptées soient prises quant à la sécurité des données biométriques enregistrées dans le passeport et qu'en particulier la transparence lors du traitement des données soit assurée.

Indépendamment de notre réponse à la consultation, nous avons rencontré à deux reprises les responsables du projet et discuté avec eux des aspects de l'introduction du passeport biométrique touchant la protection des données. En octobre 2005, nous avons eu l'occasion d'examiner sur place les systèmes de saisie biométrique présélectionnés et nous avons ainsi pu nous faire une idée plus précise de la procédure de lecture dans les centres de saisie. Durant toute la durée du projet, nous resterons en contact avec l'Office fédéral de la police, en charge du projet, et nous échangerons des informations.

3.1.6 Prolongation de deux ordonnances dans le domaine de la sécurité intérieure et extérieure

Dans le cadre de la consultation des offices, nous avons été invités à prendre position sur le projet de prolongation de deux ordonnances du Conseil fédéral dans le domaine de la sécurité intérieure et extérieure de la Suisse. Notre proposition de renoncer à la prolongation de l'ordonnance concernant l'extension du devoir de renseigner et du droit de communiquer n'a toutefois pas été suivie.

Nous avons été invités, dans le cadre d'une consultation des offices, à prendre position sur le projet de prolongation de deux ordonnances provisoires dans le domaine de la sécurité intérieure et extérieure de la Suisse qui avaient été élaborées suite aux attentats terroristes du 11 septembre 2001.

Concernant l'ordonnance interdisant le groupe «Al-Qaïda» et les organisations apparentées, nous n'avons pas eu de remarques à formuler quant à la prolongation de sa durée de validité.

En revanche, nous avons demandé de renoncer à une nouvelle prolongation de l'ordonnance concernant l'extension du devoir de renseigner et du droit de communiquer. Cette ordonnance, établie pour une durée provisoire et prolongée une première fois à fin 2003, se fonde sur la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI); elle étend le devoir de renseigner et le droit de communiquer dans le domaine de la sécurité intérieure et extérieure à tous les offices et autorités de la Confédération et des cantons, ainsi qu'à tous les établissements et organisations accomplissant des tâches de service public.

Une telle mesure représente une atteinte importante aux droits fondamentaux - notamment une atteinte généralisée au secret de fonction - et doit être pleinement justifiée.

Nous avons fait valoir que, d'une part, la législation en vigueur prévoyait déjà l'obligation de fournir des renseignements, respectivement le droit de communiquer des renseignements, pour de nombreuses autorités. D'autre part, le rapport chargé d'évaluer les résultats concrets de l'ordonnance n'avait à notre avis pas permis de démontrer la justification d'une extension du devoir de renseigner et du droit de communiquer au-delà de son seul effet théorique ou de son impact psychologique.

Bien que nous comprenions la nécessité de démontrer la volonté politique de la Suisse dans la lutte contre le terrorisme, nous avons estimé que les mesures prévues par l'ordonnance n'avaient pas atteint les objectifs visés et que les traitements de données personnelles envisagés étaient ainsi contraires au principe de proportionnalité.

En dépit de nos remarques, le Conseil fédéral a, par décision du 23 novembre 2005, prolongé les deux ordonnances précitées.

3.2 Autres thèmes

3.2.1 Révision de la législation dans le domaine de la lutte contre le blanchiment d'argent

Nous avons pris position sur deux projets de révision dans le domaine de la lutte contre le blanchiment d'argent. Nos remarques concernant la précision de la base légale n'ont pas été prises en compte et ont été mentionnées comme divergence dans la proposition au Conseil fédéral.

Nous avons été invités à prendre position sur deux projets de révision dans le domaine de la lutte contre le blanchiment d'argent. Le premier concernait l'ordonnance sur le registre de l'Autorité de contrôle en matière de lutte contre le blanchiment d'argent (Ordonnance sur le traitement des données) et le second la loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier (Loi sur le blanchiment d'argent).

S'agissant de l'ordonnance sur le traitement des données, nous avons relevé que celle-ci ne constituait pas une base légale suffisante pour la collecte de données sensibles effectuée par l'Autorité de contrôle en matière de lutte contre le blanchiment d'argent. Pour un tel traitement de données, le principe de légalité exige en effet une base légale au sens formel. En raison de l'adaptation correspondante à effectuer dans la loi sur le blanchiment d'argent, nous avons proposé d'attendre l'issue du projet de révision de cette loi avant de modifier l'ordonnance. Cette dernière est cependant déjà entrée en vigueur le 1er novembre 2005. Nos autres remarques ont, pour l'essentiel, été prises en compte.

En ce qui concerne la révision de la loi sur le blanchiment d'argent, nous avons – conformément à ce qui précède - demandé d'adapter la base légale et de préciser dans la loi l'importance et la finalité du traitement des données sensibles, comme l'exige la législation sur la protection des données.

De plus, le projet de révision désigne les autorités ayant accès au système de traitement des données GEWA. Nous avons relevé qu'il convenait également de préciser le but du traitement des données ainsi que les catégories de données traitées, en application du principe de légalité. Nous avions déjà mentionné lors de la révision de l'ordonnance sur le Bureau de communication en matière de blanchiment d'argent qu'une ordonnance ne constitue pas une base légale suffisante (voir à ce sujet notre 12ème rapport d'activités 2004/2005, chiffre 3.2.1).

Le projet de révision contient finalement une disposition selon laquelle le Bureau de communication aurait accès à la banque de données ISIS (système de traitement des données relatives à la protection de l'Etat). Nous avons estimé que la nécessité d'un tel accès n'avait pas été démontrée et nous nous sommes dès lors opposés à cette possibilité.

Nos remarques effectuées dans le cadre de la révision de la Loi sur le blanchiment d'argent n'ont pas été prises en compte et ont été mentionnées comme divergence dans la proposition au Conseil fédéral.

4 Santé

4.1 Thèmes divers

4.1.1 TARMED et protection des données

La convention-cadre TARMED requiert que la facturation entre fournisseurs de prestations et organismes payeurs soit effectuée sous forme électronique dans les deux ans qui suivent l'introduction de TARMED, c'est-à-dire depuis le 1er janvier 2006. Le passage de la facture imprimée au formulaire de facturation électronique facilite les contrôles systématiques, mais augmente également le risque d'une atteinte à la personnalité. Ce risque peut cependant être minimisé si des mesures adéquates sont prises. Nous avons consenti à aider les assureurs dans l'élaboration d'un concept de protection des données.

En prévision de l'entrée en vigueur au 1er janvier 2004 du tarif médical TARMED pour le domaine de la LAMal, nous avons procédé à deux examens des faits et publié nos constatations dans un rapport. Dans ce rapport, nous démontrons que le traitement systématique de données personnelles par les assureurs est disproportionné (cf. notre 12ème rapport d'activités 2004/2005, chiffre 5.1.1 ainsi que le rapport «TARMED et la protection des données», accessibles sur le site www.edsb.ch/f). L'introduction de la facturation électronique sans les mesures de protection nécessaires augmente le risque d'une atteinte à la personnalité.

Une des mesures de protection prescrites par la LPD est que les assureurs doivent, en leur qualité de maître de fichier, élaborer un règlement de traitement. Ce règlement définit les mesures techniques et organisationnelles permettant d'assurer un traitement des données qui soit conforme aux exigences de la protection des données.

Le traitement systématique de données sensibles exige cependant aussi une description détaillée des mesures conceptuelles qui permettent de réduire à un minimum le risque d'une atteinte à la personnalité. Le but de ces mesures est - d'une part - de protéger le patient, respectivement l'assuré. D'autre part, il s'agit de protéger les acteurs qui traitent ces données de violations du droit qui pourraient être coûteuses et pourraient nuire à leur image. Dans ce sens, le concept de protection des données joue un rôle primordial.

Nous avons accepté, dans le cadre d'une consultation, à aider les assureurs dans l'élaboration d'un concept de protection des données. Un tel concept permettra aux parties contractantes de réaliser la transparence absolument nécessaire dans le cadre d'un traitement de données personnelles sensibles.

C'est pourquoi nous avons remis aux assureurs un outil qui devrait faciliter leur familiarisation avec le sujet et les aider lors de l'élaboration d'un concept de protection des données.

4.1.2 Surveillance du respect des charges liées aux autorisations accordées dans le domaine de la recherche médicale

Le PFPD a pour tâche de contrôler l'application des charges que la Commission d'experts pour le secret professionnel dans la recherche médicale impose aux projets de recherche autorisés. Selon les contrôles effectués à ce jour, nous parvenons à la conclusion que les charges doivent être dans de nombreux cas encore mieux appliquées.

La Commission d'experts pour le secret professionnel dans la recherche médicale se prononce sur les demandes de recherches dans le domaine de la médecine ou de la santé. On distingue les autorisations particulières, établies pour des projets de recherche spécifiques, des autorisations générales, établies à l'intention des cliniques et des instituts universitaires médicaux, ainsi que des registres médicaux. Une demande d'autorisation ne doit être déposée que si la recherche ne peut pas être effectuée avec des données anonymisées, ou s'il est impossible ou particulièrement difficile d'obtenir le consentement des intéressés pour le traitement des données. Ceux-ci ont en principe le droit d'interdire l'utilisation de leurs données pour des fins de recherche et doivent être informés de ce droit de manière transparente.

Une autorisation accordée par la Commission d'experts est toujours assortie de charges, notamment:

- Les données collectées doivent être anonymisées dès que possible, mais en tout cas avant le début de l'activité de recherche proprement dite.
- Les mesures techniques et organisationnelles nécessaires à la sécurité des données doivent être prises.
- Les dossiers médicaux, y compris les fichiers informatiques, doivent être conçus de manière à ce qu'un éventuel refus de la personne concernée de mettre ses données à disposition à des fins de recherche puisse être mentionné dans les différents systèmes d'information.

Une fois que la Commission d'experts a autorisé la levée du secret professionnel, nous avons pour tâche de surveiller le respect des charges assorties à cette autorisation. Lors de nos contrôles, nous nous concentrons sur la phase de la collecte des données jusqu'à leur anonymisation, car il s'agit alors d'un traitement de données personnelles au sens de la LPD – à savoir des indications sur des personnes identifiées ou identifiables. Avant d'effectuer un contrôle sur place, nous exigeons de la part des titulaires de l'autorisation un document présentant de manière détaillée le flux des informations, ainsi que les processus et les mesures de sécurité des données. Par ailleurs, nous contrôlons aussi l'information faite aux intéressés sur leur droit de blocage, ainsi que la mise en œuvre de ce droit. D'autres charges, notamment celles qui sont spécifiques aux diverses recherches, sont également contrôlées.

Lors de plusieurs contrôles, nous avons constaté que la documentation n'était pas suffisamment complète. Les mesures de sécurité des données n'ont dans certains cas pas été appliquées ou l'ont été de façon insuffisante. La mise en œuvre du blocage des données n'a jamais été entreprise dans les différents systèmes contrôlés. Selon les motifs avancés, les patients n'auraient encore jamais fait valoir leur droit de blocage. Vu les insuffisances constatées lors de nos contrôles, nous estimons nécessaire de poursuivre nos activités de surveillance dans ce domaine.

4.1.3 Droit applicable aux services Spitex

Les traitements de données par les services Spitex sont-ils soumis au droit fédéral de la protection des données ou au droit cantonal de la protection des données? Selon l'avis rédigé à ce sujet par l'Office fédéral de la justice, le traitement de données par les services Spitex est en général soumis à la surveillance des autorités cantonales de protection des données.

En Suisse, les services d'aide et de soins à domicile sont dispensés par les différents services Spitex. L'Association suisse des services d'aide et de soins à domicile, association faîtière qui représente les services Spitex, envisage d'introduire pour toute la Suisse un système d'assurance qualité, le RAI-domicile Suisse. Une question controversée se pose à ce sujet: l'introduction du modèle RAI-domicile Suisse relève-t-elle du droit fédéral sur la protection des données ou du droit cantonal sur la protection des données? Cette question en implique une autre: le traitement de données effectué par les services Spitex est-il soumis à la surveillance du préposé fédéral à la protection des données (PFPD) ou à celle des préposés cantonaux à la protection des données?

Si l'on considère que les services Spitex sont des institutions privées dont les actes relèvent du droit privé et qui ne constituent donc pas une autorité disposant de la puissance publique, c'est la loi fédérale sur la protection des données qui est applicable et, de ce fait, le PFPD est l'autorité de surveillance compétente. Par contre, si l'on estime que les services Spitex remplissent des tâches cantonales et exercent une puissance publique fondée sur les lois cantonales, il s'ensuit que le droit cantonal de la protection des données est applicable. Le traitement de données par les services Spitex est alors soumis à la surveillance des préposés cantonaux à la protection des données.

Nous avons donc prié l'Office fédéral de la justice (OFJ) de rédiger un avis sur cette question de compétence. L'OFJ estime que les soins dispensés à domicile constituent une tâche publique des cantons et des communes. Par ailleurs, les services Spitex sont subventionnés par les cantons et les communes, sur mandat desquels ils agissent. Enfin, l'OFJ a précisé que ces services étaient soumis à la surveillance des autorités cantonales et communales, donc que les autorités cantonales de protection des données sont chargées de surveiller les traitements de données effectués par les services Spitex.

Tout comme l'OFJ, nous estimons que la surveillance au titre de la protection des données des services Spitex incombe aux cantons. Le système d'assurance qualité RAI-domicile Suisse doit donc être adapté en fonction des normes cantonales de protection des données.

4.1.4 Les biobanques: entre les intérêts de la recherche et la protection de la personnalité

Les biobanques rassemblent une multitude de données sur une personne. Outre les données concernant la santé et le style de vie, elles contiennent aussi du matériel biologique (sang, ADN, tissus, lignages cellulaires) qui est ensuite traité pour la recherche. Comment agir en présence de matériel biologique et quelles exigences poser au consentement de la personne concernée sans entraver complètement la recherche? Comment empêcher une utilisation abusive des données (génétiques) obtenues? Nous avons pris part à diverses rencontres au cours desquelles ces questions ont été soulevées. L'Académie suisse des sciences médicales (ASSM) a élaboré des directives qu'elle a envoyées en consultation. Ces directives accordent une grande importance à la protection des données et de la personnalité dans le cas des biobanques.

Les biobanques existent dans le monde entier et sont de plus en plus nombreuses. Elles permettent aux chercheurs de faire des rapprochements entre la constitution génétique et les maladies. Les hôpitaux rassemblent aussi du matériel biologique et des données de patients qui sont utilisés par la suite pour la recherche. Nous avons participé à diverses rencontres consacrées aux biobanques, dont une organisée par la Fondation pour la protection des données et la sécurité de l'information, GenSuisse et OncoSuisse. Ces rencontres ont été pour nous l'occasion de nous exprimer sur la question du consentement des patients et sur le traitement subséquent du matériel biologique et des données personnelles.

Les données relevées à des fins de recherche ne doivent être traitées qu'avec le consentement de la personne concernée. En principe, cette règle vaut également une fois le projet concret de recherche achevé. Mais c'est justement là qu'est le problème: souvent, au début d'un projet de recherche, on ne sait pas très bien où la recherche va mener et quelles connaissances supplémentaires pourront être obtenues. Dans certains cas, il est également difficile, voire même impossible d'obtenir le consentement des patients concernés pour d'autres projets de recherche, par exemple parce que le recueil des données a eu lieu il y a déjà des années ou parce qu'on ne veut plus confronter le patient avec une maladie. Certains sont aussi d'avis qu'il n'est pas nécessaire d'avoir le consentement exprès du donneur, mais qu'il convient de préférer la solution dite de l'opposition: celui qui ne veut pas que son matériel biologique soit utilisé par un laboratoire doit expressément s'y opposer.

A cet égard, nous avons adopté une attitude plutôt restrictive et demandé que le matériel biologique et les données personnelles qui en font partie ne soient en principe traités qu'avec le consentement exprès de la personne concernée. Ce consentement ne doit pas se limiter à un projet de recherche spécifique, mais peut se référer à un domaine de recherche prédéfini. Par contre, un consentement général pour toute recherche future qui serait donné au moment du prélèvement des données serait à nos yeux disproportionné. Il convient en outre de requérir que toutes les données soient anonymisées ou pseudonymisées le plus tôt possible. La pseudonymisation devrait avoir lieu de préférence par double codage et la clé de codage devrait être déposée auprès d'une institution indépendante.

Les directives de l'ASSM, au sujet desquelles nous nous sommes exprimés à l'occasion de la consultation, vont dans la même direction. D'une manière générale, nous avons entièrement approuvé la création de ces directives médicoéthiques qui devraient guider les personnes qui gèrent les biobanques et leurs utilisateurs jusqu'à ce qu'une base légale soit élaborée au niveau fédéral. Cela dit, nous avons suggéré que la définition de la notion de biobanques précise clairement que ces dernières rassemblent des données personnelles sensibles au sens de l'art. 3, let. c, ch. 3 LPD. Nous avons également spécifié que les biobanques sont soumises aux règles de droit cantonales, fédérales et constitutionnelles en vigueur. En outre, le but d'une biobanque doit être défini avec la plus grande précision possible. Nous avons constaté avec satisfaction que le consentement exprès a été établi comme principe. Toutefois nous n'avons partagé la conception selon laquelle l'accord du patient sous forme de consentement général est exceptionnellement permis. Comme nous l'avons déjà exposé, nous pourrions considérer comme suffisant un consentement plus large au traitement de données dans le cadre d'un projet de recherche prédéfini (comme les maladies tumorales, la pharmacogénétique).

Nous participerons en outre à la procédure de consultation concernant la loi fédérale relative à la recherche sur l'être humain (LHR) qui réglera la question des biobanques au niveau suisse.

Les directives de l'ASSM peuvent être consultées sur Internet à l'adresse www.samw.ch.

4.1.5 La banque de données sur la valeur intrinsèque

La loi sur l'assurance-maladie (LAMal) prévoit que la convention-cadre TARMED peut soumettre, à titre exceptionnel, en vue de garantir leur qualité, la rémunération de certaines prestations à des conditions précises. Il s'agit notamment de l'existence de l'infrastructure nécessaire ainsi que de la formation de base, de la formation postgraduée ou de la formation continue du prestataire de services. Dans cette convention-cadre, les partenaires tarifaires ont convenu que la FMH détiendrait une banque de données devant permettre aux assureurs d'accéder par voie électronique aux informations dont ils ont besoin (banque de données sur la valeur intrinsèque). Dans ce cadre, la FMH nous a soumis pour appréciation un concept de mise en œuvre. Nous sommes arrivés à la conclusion que la banque de données sur la valeur intrinsèque ne viole en principe la LPD, même si elle nécessite quelques adaptations.

Dans la convention-cadre TARMED, les partenaires tarifaires ont convenu que la Fédération des médecins suisses FMH permettrait aux assureurs d'accéder par voie électronique aux données de valeur intrinsèque de leurs membres. Les données devant être traitées sont le numéro EAN, le nom et le prénom du prestataire de services, ses diplômes ainsi que la garantie des droits acquis pour TARMED. Le concept qui nous a été soumis par la FMH prévoit que la banque de données sur la valeur intrinsèque soit transmise intégralement aux assureurs.

Cet état de faits soulève les questions suivantes: La FMH viole-t-elle la LPD si elle traite les données conformément à ce concept? Si tel était le cas, quelles mesures la FMH doit-elle prendre pour éviter ceci?

Dans la banque de données sur la valeur intrinsèque, la FMH traite des données personnelles. Il n'y a pas d'atteinte illicite à la personnalité si le traitement est justifié par une loi. Dans le cas présent, l'exigence du législateur formulée à l'article 43, alinéa 2, lit. d de la LAMal représente un motif justificatif. Celui-ci permet, à titre exceptionnel, de rendre accessibles à l'assureur les données sur la valeur intrinsèque d'un prestataire de services dans le but prévu par le législateur. Cependant, la transmission à l'assureur de l'intégralité des données sur la valeur intrinsèque viole le principe de proportionnalité.

Nous avons pour cette raison demandé à la FMH de réviser son concept de manière à ce que la vérification de la valeur intrinsèque par les assureurs ne soit effectuée que pour les prestations prévues par la loi. La FMH doit en outre prendre les mesures permettant d'éviter que des données sur la valeur intrinsèque soient mémorisées auprès des assureurs ou que les assureurs concernés puissent créer une copie de la banque de données de la FMH.

Nous vérifierons à l'avenir si nos exigences ont été respectées.

4.1.6 La sécurité des données dans un cabinet médical

L'ordinateur est devenu un élément essentiel d'un cabinet médical, d'autant plus que les prestations médicales doivent être facturées électroniquement depuis 2006. L'introduction prévue de la carte d'assuré favorise également fortement ce développement. Les demandes que nous avons reçues montrent qu'il existe une certaine insécurité au sein des fournisseurs de prestations concernant la question de savoir comment permettre au cabinet médical de recourir au traitement électronique tout en assurant une protection suffisante. Parmi les solutions possibles, on compte la séparation des données, de manière logique ou physique.

De nos jours, l'ordinateur est devenu un outil de travail commun dans un cabinet médical, notamment à cause de la facturation électronique qui, avec la convention-cadre TARMED, est devenue obligatoire à partir de 2006. Une application importante à l'avenir sera la carte d'assuré pour les ressortissants suisses. Dans ce contexte, les prestataires de services doivent se poser la question suivante: dans quelles conditions est-il permis de stocker des données sensibles sur un ordinateur relié à Internet? Si l'on n'attache pas une importance primordiale à cette question, cela peut avoir des conséquences catastrophiques. Il n'est pas exclu que, suite à un accès illicite aux données d'un patient – rendu possible par des liaisons non sécurisées – le patient subisse une atteinte illicite à sa personnalité et que le médecin doive se justifier pour violation du secret médical, ce dernier constituant un délit.

Pour éviter ceci, les données des patients doivent être protégées de sorte qu'il ne soit pas possible d'y accéder par Internet, par quelque moyen que ce soit.

Cette protection peut être réalisée de deux manières. La première consiste à installer un système pare-feu, matériel ou logiciel. La deuxième solution est encore plus sûre: les données sont isolées d'Internet, de manière logique ou physique. Dans le cas d'un isolement logique, les données sont bel et bien stockées sur l'ordinateur relié à Inter-

net, mais elles sont présentes sur le support de stockage (par ex. sur le disque dur) sous forme cryptée. Dans le cas d'un isolement physique, les données sont stockées sur un ordinateur séparé, qui n'est pas connecté à Internet. La deuxième possibilité offre une protection maximale.

4.2 Génétique

4.2.1 Ordonnance relative à la loi sur l'analyse génétique humaine

Le 8 octobre 2004, le Parlement a adopté la loi fédérale sur l'analyse génétique humaine (LAGH). Son entrée en vigueur est prévue, avec les dispositions d'exécution, pour l'été 2006. L'ordonnance règle les conditions et la procédure d'octroi des autorisations en vue de la réalisation des analyses génétiques. Dans le cadre de la consultation des offices, nous nous sommes prononcés sur la durée de conservation des données personnelles, sur la sécurité des données et sur la transmission de matériel biologique et de données personnelles.

Le fait que les laboratoires soient tenus de conserver pendant 30 ans au moins les résultats des analyses génétiques (rapports d'analyse) nous a semblé problématique. Ces rapports d'analyse contiennent les résultats des analyses génétiques de patients. Ces données portant sur la constitution génétique des personnes concernées sont, du point de vue du droit de la protection des données, des données personnelles sensibles (données médicales particulièrement dignes de protection) conformément à l'art. 3 lit. c, ch. 2 LPD. Conformément au principe de la proportionnalité, la durée de conservation des données personnelles doit tenir compte, dans un rapport raisonnable, du but visé par le traitement.

Cela ne peut être la tâche des laboratoires de conserver les rapports d'analyse contenant des données personnelles sensibles pour la génération suivante. A notre avis, une obligation de conserver ces données pendant 30 ans (et non plus, comme il était prévu auparavant, pendant *au moins* 30 ans) est proportionnée. En outre, nous avons demandé de garantir que les rapports ne soient pas utilisés de façon abusive et qu'ils ne soient pas remis à des tiers non autorisés. Pour cette raison, nous avons proposé d'ajouter un passage précisant que les laboratoires sont tenus, à l'aide de mesures techniques et organisationnelles, de veiller à ce que les dossiers soient suffisamment protégés contre tout accès indu.

Enfin, nous avons demandé que les données des patients et le matériel biologique ne soient communiqués à un autre laboratoire dans le cadre d'un mandat exécuté en sous-traitance que sous une forme pseudonymisée.

5 Assurances

5.1 Assurances sociales

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

Dans le cadre de la révision de la loi fédérale sur l'assurance-maladie, le législateur a créé les bases légales pour l'introduction de la «carte d'assuré» en Suisse. L'office fédéral de la santé publique a été chargé d'élaborer les bases pour l'introduction de cette carte. Nous accompagnons le projet depuis qu'il a été lancé.

A l'article 42a de la loi fédérale révisée sur l'assurance-maladie (LAMal), le législateur donne au Conseil fédéral la possibilité d'introduire des cartes d'assuré pour toutes les personnes soumises à l'assurance-maladie obligatoire.

Cette carte contient le nom de la personne assurée ainsi qu'un numéro d'assurance sociale attribué par la Confédération. La carte est utilisée pour facturer les prestations fournies dans le cadre de cette loi. Outre cette partie obligatoire de la carte d'assuré, le Conseil fédéral peut fixer l'étendue des données personnelles qui peuvent, avec le consentement de la personne assurée, être enregistrées sur la carte.

Comme dans de nombreux projets dans les domaines de la santé publique et des assurances, le projet d'introduction de la carte d'assuré se voit confronté à diverses exigences conflictuelles. Alors que certains demandent qu'un maximum d'informations soit mémorisé sur la carte, d'autres exigent que seules les informations absolument nécessaires soient disponibles sur la carte. Ainsi, nous avons également toujours défendu la position que cette carte ne devait, dans son utilisation obligatoire, contenir que les données exigées par le législateur, à savoir le nom de la personne assurée et son numéro d'assuré. En outre, ces données ne doivent à notre avis être utilisées que pour le but prévu par la loi, à savoir pour la facturation. Nous avons réussi, après plusieurs interventions, à faire accepter ces exigences.

Pour l'usage facultatif, les conditions sont différentes. Dans un concept préliminaire, l'Office fédéral de la santé publique (OFSP) propose les applications suivantes: indications relatives aux assurances complémentaires, données cliniques limitées, médication actuelle, ordonnance électronique et projets modèles cantonaux. La LPD prévoit que des données personnelles sensibles peuvent exceptionnellement être traitées dans les cas où la personne concernée a, en l'espèce, donné son consentement ou

rendu ses données accessibles à tout un chacun (art. 17 al. 2, lit. c LPD). Ceci est le cas pour les applications prévues. Nous exigeons cependant qu'une condition importante soit remplie: si la personne concernée refuse de donner son consentement, elle ne doit pas subir de préjudices. Ainsi, il n'est pas admissible par exemple d'exiger de l'assuré qu'il donne son consentement à l'ordonnance électronique pour pouvoir bénéficier d'une réduction de primes.

Un autre problème relatif à l'introduction de la carte d'assuré est celui du numéro d'assurance sociale. Il est prévu non seulement que ce ce numéro soit enregistré électroniquement sur la carte, mais qu'il soit également imprimé de manière bien visible. Cela signifie que toute personne qui voit la carte pourra sans autre associer ce numéro avec la personne assurée. L'exigence selon laquelle ce nouveau numéro d'assurance sociale ne peut pas – contrairement au numéro AVS – permettre d'identifier la personne concernée est sérieusement compromise. Ceci est d'autant plus vrai qu'il est prévu d'utiliser le numéro d'assurance sociale également dans des domaines qui n'ont rien à voir avec l'assurance sociale, tel que le recensement de la population (cf. chiffre 1.2.1 du présent rapport d'activités).

5.1.2 La 5ème révision de l'assurance-invalidité

Dans le cadre de la consultation des offices sur la 5ème révision de l'AI, nous nous sommes à nouveau prononcés sur des questions relevant de la protection des données. Le Conseil fédéral a adopté le message ainsi que le texte de loi. Néanmoins, le message n'est pas satisfaisant du point de vue de la protection des données. La 5ème révision de l'AI est actuellement en suspens devant le parlement.

La 5ème révision de l'AI a pour objectif principal d'améliorer les mesures de détection et d'intervention précoces dans le domaine de l'AI. Une action d'ensemble dans le domaine médical, social et professionnel devrait permettre aux personnes concernées de rester dans le circuit du travail. Ceci aurait cependant pour conséquence une augmentation des données traitées entre autres par l'employeur, l'assureur d'indemnités journalières, l'Office AI et le médecin.

Dans le cadre de la consultation des offices, nous avons une fois encore souligné les exigences légales en matière de protection des données auxquelles est soumis le traitement de données personnelles sensibles (données médicales; voir également notre 12ème rapport d'activités 2004/2005, chiffre 6.1.2).

Nous avons constaté avec satisfaction que le Conseil fédéral a pris au sérieux nos préoccupations concernant le manque de transparence du traitement des données. Ainsi, le dernier projet prévoit un renforcement du devoir d'information à l'égard des personnes concernées, c'est-à-dire les assurés.

Par contre, un point demeure insatisfaisant: selon le projet de message, les personnes assurées ne seront pas les seules à pouvoir s'annoncer en vue de la détection précoce auprès de l'Office AI. Plusieurs autres personnes, dont l'assureur, l'employeur, un membre de la famille ou le service d'aide sociale, peuvent aussi annoncer la personne assurée auprès de l'Office AI. Mais la situation devient délicate lorsque l'employeur consulte les données concernant l'employé, données auxquelles il n'aurait normalement pas accès. Il en résulte un risque de discrimination potentielle sur le lieu de travail. Sur la base du principe d'autodétermination en matière d'information, c'est à la personne concernée de décider elle-même et librement du traitement des données la concernant. Le fait de s'annoncer volontairement n'est pas seulement un élément essentiel du principe d'autodétermination en matière d'information, c'est également une condition inséparable d'une relation de confiance entre l'Office AI et la personne assurée.

Enfin, la 5ème révision de l'AI prévoit une autorisation générale pour l'examen du droit aux prestations. Une telle procuration en blanc ne devrait pas seulement permettre aux offices AI de collecter des données, mais aussi à tous les assureurs sociaux. Nous avons précisé plusieurs fois que ce genre de procuration générale n'est pas compatible avec la législation sur la protection des données. Le consentement doit se donner au cas par cas et la personne concernée doit être informée en détail sur la portée et le but de son consentement.

Les questions relevant des aspects légaux de la protection des données en relation avec la révision de la 5ème révision de l'AI ont été ensuite traitées par la Commission de la sécurité sociale et de la santé publique du Conseil national (CSSS-N). Nous avons été invités par la CSSS-N à présenter notre point de vue. Il n'est, dans l'état actuel des choses, pas possible de dire quel projet sera approuvé par les Chambres fédérales.

5.1.3 Les assureurs-maladie sociaux et le devoir légal de discrétion

Nous avons appris qu'à plusieurs reprises, des assureurs-maladie sociaux avaient transmis des données d'assurés à un centre de cardiologie. Rappelons à ce propos que les assurances-maladie sont en principe soumises au devoir légal de discrétion.

Plusieurs personnes ont été contactées par un centre de cardiologie pour savoir si elles étaient prêtes à participer à un programme consacré aux personnes atteintes de maladies cardiaques. Selon les affirmations des personnes concernées, plusieurs caisses-maladie auraient communiqué au centre de cardiologie quels patients prenaient quel médicament. Dans un cas au moins, l'affaire a été portée devant l'autorité de surveillance compétente, l'Office fédéral de la santé publique, auprès duquel elle est encore pendante.

Nous avons conseillé les patients concernés et nous sommes arrivés à la conclusion suivante«la loi fédérale sur la partie générale du droit des assurances sociales prévoit que l'assureur social doit garder le secret à l'égard de tiers. Les exceptions à cette obligation légale de garder le secret sont réglées dans les divers textes de loi concernant les assurances sociales. D'après ces textes, les assureurs-maladie sociaux sont soumis aux dispositions de la loi sur l'assurance-maladie (LAMal).

Dans le cas présent, la LAMal ne prévoit pour les assureurs-maladie qu'une seule possibilité de transmission de données d'assurés à des tiers: ces données ne peuvent être communiquées à des tiers que lorsque la personne concernée y a, dans le cas d'espèce, consenti par écrit (cf. art. 84a al. 5, let. b LAMal). Etant donné qu'il s'agit ici

de données personnelles sensibles (données médicales), il convient de formuler des exigences particulièrement élevées s'agissant de la portée et de la finalité du consentement. Par ailleurs, il faut veiller à ce que seules les données nécessaires soient transmises à des tiers.

Si le consentement écrit de la personne concernée n'est pas donné, on peut considérer qu'il y a atteinte illicite à la personnalité. Cette personne peut utiliser les voies de droit prévues par la législation sur la protection des données, par exemple les actions en dommages-intérêts et en réparation du tort moral. Enfin, elle peut déposer une plainte pénale auprès des autorités cantonales compétentes. Toute personne violant l'obligation de discrétion en tant qu'organe d'exécution au sens de la LAMal est en effet passible d'une peine d'emprisonnement ou d'une amende.

5.2 Assurances privées

5.2.1 La collecte de données personnelles par les assurances-responsabilité civile

Une compagnie d'assurance-responsabilité civile a mis au point un concept pour la collecte de données sur des personnes lésées. Dans cette optique, elle a élaboré une notice consacrée à la protection des données ainsi qu'une clause de consentement.

Une compagnie d'assurance-responsabilité civile a mis au point une notice d'information destinée aux médecins et aux hôpitaux afin d'attirer leur attention sur la loi sur la protection des données ainsi que sur le secret médical fixé dans le droit pénal. Selon cette notice, le consentement écrit du patient doit être donné pour que le médecin soit délivré du secret médical à l'égard de l'assureur responsabilité-civile; si le patient ou la personne lésée ne donne pas son consentement, l'assureur-responsabilité civile ne peut traiter le cas car les données du patient ne devraient pas lui être transmises.

La déclaration de libération du secret médical contient les noms de la personne lésée, du médecin traitant ainsi que la finalité de cette libération (traitement/opération). De plus, la clause de consentement a pour but de délivrer du secret médical tous les autres médecins impliqués, le personnel médical et le personnel administratif. En outre, elle a pour but d'autoriser l'assureur-responsabilité civile à consulter les dossiers des assurés sociaux et privés.

Il faut en principe approuver la démarche de l'assureur-responsabilité civile visant à soumettre la collecte de données émanant du médecin traitant et concernant le patient au consentement écrit de celui-ci. Ce consentement est notamment nécessaire pour libérer le médecin du secret médical conformément à l'art. 321 CP. Toutefois la clause de consentement doit être améliorée dans la mesure où elle s'applique également à d'autres médecins, assureurs privés, etc. En effet, il n'est pas clairement dit auprès de qui l'assureur-responsabilité civile ira chercher quelles données personnelles et dans quel but. Or le degré de concrétisation du consentement doit répondre à des exigences d'autant plus élevées qu'il s'agit de données personnelles sensibles (en l'espèce, de données médicales).

Il serait également souhaitable que cette notice d'information sur la protection des données ne soit pas envoyée aux seuls médecins, mais aussi et surtout aux personnes directement concernées. En effet, ce sont essentiellement les données des personnes lésées qui sont traitées (voir à ce sujet notre 11ème rapport d'activités 2003/2004, chiffre 6.2.1 et annexe 13.4).

5.2.2 Lutte contre l'escroquerie en matière d'assurance automobile

Plusieurs compagnies suisses d'assurance ont l'intention de mettre en place un système commun visant à détecter les cas d'escroquerie en matière d'assurance automobile. Leur objectif est de détecter le plus tôt possible les cas d'escroquerie ou leurs actes préparatoires et de les empêcher en enquêtant sur des sinistres antérieurs ou déjà annoncés. Afin de compléter les fichiers et d'améliorer leur efficacité, ces assureurs envisagent de saisir également les données concernant le calcul des dommages effectué par les garagistes. Or, cela suppose dans certains cas que les instances de calcul en soient informées au préalable et qu'elles donnent leur consentement.

Sur mandat de plusieurs assureurs suisses, une entreprise zurichoise (ci-après l'entreprise responsable) élabore actuellement un système de détection des cas d'escroquerie en matière d'assurance automobile. Elle nous a demandé d'apprécier ce système à la lumière des prescriptions en matière de protection des données.

Il est prévu que le système fonctionne comme suit: les assureurs, les experts et les garagistes reçoivent de l'entreprise responsable un logiciel permettant de calculer le coût des dommages causés aux véhicules. Ils saisissent leurs données de calcul dans

une banque de données centrale (ci-après la banque de données de calcul). Cette banque, qui est exploitée par l'entreprise responsable, a pour objectif premier l'établissement des factures à l'intention de ces instances de calcul.

Au cours d'une seconde phase, les données de calcul centralisées sont transférées de la banque de données de calcul dans une seconde banque de données. Cette seconde banque de données abrite le véritable système de détection des cas d'escroquerie, dénommé *Vehicle Claim History System* (ci-après système de détection des cas d'escroquerie). Cette banque de données indique pour chaque sinistre essentiellement le numéro du châssis, le code de la compagnie d'assurance, le montant des dommages et la date des calculs.

Selon les précisions fournies par l'entreprise responsable, le système de détection des cas d'escroquerie recevra aussi les données des instances de calcul qui utilisent exclusivement le logiciel de calcul des dommages et la banque de données de calcul.

Du point de vue du droit de la protection des données, les remarques suivantes s'imposent: le numéro de châssis d'un véhicule permet de mettre en relation les données contenues dans le système de détection des cas d'escroquerie, avec les recueils de données de clients des assurances tout comme avec la banque de données de calcul. Il convient donc de considérer le numéro de châssis comme une donnée personnelle, au sens de la LPD. En effet, il permet aux différentes instances de calcul et à l'entreprise responsable du système de déterminer les propriétaires actuels et antérieurs d'un véhicule. La LPD est donc applicable à la fois au système de détection des cas d'escroquerie et à la banque de données de calcul.

La LPD s'applique donc sur trois niveaux différents: au niveau des instances de calcul qui participent au système de détection des cas d'escroquerie, au niveau de celles qui n'y participent pas, et enfin au niveau des preneurs d'assurance.

En ce qui concerne les instances de calcul participant au système de détection des cas d'escroquerie, il n'est pas nécessaire de requérir leur consentement pour traiter les données de calcul car la lutte contre l'escroquerie constitue pour elles un intérêt prépondérant.

Pour ce qui est des instances de calcul ne participant pas au système de détection des cas d'escroquerie, leur nom ne doit pas être mis à la disposition de tiers par procédure d'appel dans la banque de données mentionnée. Ces instances de calcul doivent donc demeurer anonymes. Mais comme leur nom est connu au sein de l'entreprise responsable, le traitement de leurs données de calcul dans le système de détection des cas d'escroquerie présuppose un consentement éclairé, libre et exprès en vue

du traitement supplémentaire. Ce consentement doit à son tour se fonder sur l'information préalable des instances de calcul. Si ces conditions ne sont pas remplies, non seulement il y a violation du principe de bonne foi, mais aussi violation du principe de finalité, selon lequel les données personnelles ne doivent être traitées que pour le but indiqué lors de leur collecte, prévu par une loi ou ressortant des circonstances.

Enfin, les preneurs d'assurance doivent être informés de manière appropriée par l'entreprise responsable et par les différentes instances de calcul du système de détection des cas d'escroquerie et des traitements de données y relatifs (en particulier de l'échange de données entre les assurances et les garages). Cette mesure permettra non seulement de garantir la transparence du système de détection des cas d'escroquerie, mais aussi le droit d'accès à l'information des propriétaires de véhicules. En outre, un propriétaire de véhicule ayant un intérêt avéré à cette recherche - par exemple en cas d'achat prochain d'une voiture - doit pouvoir, par exemple par l'intermédiaire du garage, accéder au système de détection des cas d'escroquerie pour vérifier si le véhicule a déjà subi des accidents.

Nous avons encore attiré l'attention de l'entreprise responsable sur les principes du droit de la protection des données, pertinents pour le système de détection des cas d'escroquerie:

Le respect du principe de proportionnalité, selon lequel seules les données qui sont nécessaires et appropriées à l'accomplissement du but indiqué doivent être traitées, ne s'impose pas seulement au niveau de l'exploitation de la banque de données de calcul et du système de détection des cas d'escroquerie, mais aussi des flux de données entre les différentes instances participantes (par ex. en cas d'échange par téléphone d'informations entre garages et assurances). Les assurances sont du reste liées par leurs obligations spécifiques de confidentialité à l'égard de tiers.

Il convient de garantir que les conditions de la LPD sont remplies également lorsque les clients sont à l'étranger.

Tant l'entreprise responsable que les instances de calcul impliquées doivent mettre en œuvre les mesures techniques et organisationnelles les plus récentes afin de se protéger contre les traitements de données indus.

6 Secteur du travail

6.1 La recherche de renseignements concernant la solvabilité des employés

De plus en plus souvent, la solvabilité des employés est contrôlée dans le cadre des rapports de travail. Un extrait du registre des poursuites ne peut être requis que s'il permet d'apprécier l'aptitude d'un candidat à occuper un poste et si un intérêt particulier, actuel et digne de protection le justifie.

Une grande entreprise suisse nous a contactés pour savoir s'il était licite de demander systématiquement un extrait du registre des poursuites d'un candidat ou d'un employé. Après examen de la doctrine et de la pratique et en tenant compte en particulier des principes du droit des poursuites et du droit de la protection des données, nous avons transmis l'avis suivant à l'entreprise:

La loi fédérale sur la poursuite pour dettes et la faillite (LP) soumet l'obtention d'un extrait du registre des poursuites à l'existence d'un intérêt particulier, actuel et digne de protection. Cet intérêt ne doit pas nécessairement être de nature financière, un autre intérêt juridique suffit aussi. Le requérant peut aussi consulter le registre sans preuve stricte de cet intérêt, lorsque des indices sérieux rendent l'existence de ce dernier vraisemblable.

Dans la pratique, un intérêt digne de protection est généralement reconnu pour les requérants pouvant prouver ou du moins rendre vraisemblable qu'ils ont une créance envers la personne sur laquelle ils désirent se renseigner. En outre, ce qui est encore plus fréquent, on reconnaît un intérêt à l'appréciation de la solvabilité d'une personne lorsque le requérant peut prouver ou rendre vraisemblable qu'un contrat est sur le point d'être conclu ou qu'une procédure judiciaire avec la personne en question est pendante. Avec ce droit d'accès prévu par la LP, le législateur a considéré dans un tel cas l'intérêt au secret de la personne concernée moins important que l'intérêt à l'information de tiers.

Pour qu'il y ait intérêt digne de protection, il doit y avoir un lien direct entre l'information sur la solvabilité et la mise en danger des intérêts légitimes de la personne qui demande les renseignements. Dans de nombreux cas, ce rapport est manifeste, par exemple dans le cas de l'octroi d'un crédit. Un lien direct semble tout aussi manifeste dans le cas d'un propriétaire qui examine la solvabilité d'un locataire potentiel.

Dans le cas d'un rapport de travail, il n'y a généralement pas d'intérêt légitime à l'information. Mais là aussi, il peut exister des cas où une demande de renseignements se justifie, par exemple lorsque l'employé est appelé à occuper un poste de confiance, comme la gestion de fonds de la clientèle ou la gestion de caisses et de coffres. Dans ce cas, l'insolvabilité personnelle d'un candidat ou d'un employé peut constituer une mise en danger des intérêts de l'employeur.

6.2 Procédure d'admission auprès d'une caisse de pension

Dans le cadre de la procédure d'admission auprès d'une caisse de pension, des données sur la santé sont en principe recueillies. Au cours de l'année écoulée, nous avons rencontré plusieurs cas dans lesquels il n'était pas clair qui était habilité à traiter quelles données personnelles.

Plusieurs personnes nous ont contactés, dans le cadre de leur procédure d'admission auprès d'une caisse de pension, pour nous demander conseil. Nous avons procédé à quelques investigations, surtout auprès de deux grandes entreprises, et nous sommes parvenus aux conclusions suivantes:

Lorsqu'une personne commence un nouvel emploi, elle doit en général faire une demande pour être admise auprès d'une caisse de pension. Elle doit à cet effet remplir des formulaires standard comportant des questions sur son état de santé. Parfois, elle peut même être invitée à consulter un médecin. Il s'agit en général du médecin-conseil ou du représentant du service médical de la caisse de pension.

Dans le cadre de la prévoyance obligatoire, la caisse de pension est obligée d'admettre la personne concernée, indépendamment de son état de santé. Si la caisse de pension offre des prestations qui vont au-delà du domaine obligatoire, ce qui est la plupart du temps le cas, les examens médicaux sont en principe autorisés. Il convient néanmoins de veiller à ce que seules les données personnelles nécessaires et appropriées au but poursuivi ne soient traitées (principe de proportionnalité).

Ce principe s'applique en particulier aux questions ou aux examens sur l'état de santé permettant à l'institution de prévoyance d'émettre une réserve de cinq ans maximum. On constate, hélas, que les questionnaires sur la santé ont tendance à devenir de plus en plus volumineux et détaillés. Il est donc d'autant plus important que les données médicales de la personne faisant une demande d'admission demeurent auprès du service médical. Une transmission des données à l'institution de prévoyance est disproportionnée et ne serait de toute manière autorisée qu'avec le consentement exprès de la personne concernée.

Nous estimons par ailleurs que le médecin compétent de l'institution de prévoyance ne peut transmettre à autrui les informations sur une éventuelle réserve que dans la mesure du nécessaire. En aucun cas il ne faut communiquer à l'employeur une éventuelle réserve dans le cadre de la procédure d'admission, sans parler d'autres données concernant la santé du requérant. Il convient en particulier de veiller à ce que l'employeur n'ait pas accès au questionnaire concernant l'état de santé.

Enfin, le requérant doit être informé en détail du contenu et du but du traitement de ses données (principe de transparence). Il doit notamment savoir avec précision qui traite quelles données personnelles dans le cadre d'une procédure d'admission dans la caisse de pension. Le devoir d'information concernant le traitement des données est également valable lorsque l'employeur ou son médecin-conseil désire enquêter sur l'aptitude au travail du candidat. Là aussi, il est important qu'aucune donnée médicale ne tombe entre les mains de l'employeur. Celui-ci ne peut être informé que sur le degré d'aptitude à remplir la tâche en question. Dans la pratique, il est souvent difficile de savoir qui traite quelles données et dans quel but.

6.3 Utilisation du GPS dans les véhicules de service

Dans le domaine du travail, l'utilisation de la technologie GPS (*Global Positioning System*) permet de visualiser en permanence les coordonnées des véhicules de service et sert essentiellement à contrôler les prestations des collaborateurs en service à l'extérieur. Du point de vue de la protection de la personnalité et de la santé, cette mesure ne pose en principe aucun problème pour autant que le principe de proportionnalité soit respecté.

L'employé d'une entreprise de montage de l'agglomération genevoise nous a contactés en se plaignant que son employeur avait équipé tous les véhicules de service d'une installation GPS. Il se sent offensé et atteint dans sa personnalité. Il nous a donc demandé de rendre un avis juridique sur la question. Après examen des faits et de la jurisprudence y relative, nous sommes parvenus aux conclusions suivantes:

Dans le domaine du travail, le GPS sert principalement à contrôler les performances des collaborateurs en service à l'extérieur, mais aussi à localiser les véhicules volés. Le relevé du tracé des véhicules de service a lieu systématiquement lors de chaque déplacement du véhicule en dehors de l'entreprise. En outre, ce relevé est permanent car il peut couvrir toute la journée de travail et même parfois la nuit. Enfin, il peut être ciblé lorsque les données relevées sont effectivement exploitées à des fins de contrôle des performances.

L'utilisation d'un GPS a une incidence sur le droit de la protection de la personnalité lorsqu'il permet d'établir un profil des déplacements des collaborateurs en service à l'extérieur.

A la différence du contrôle systématique du comportement, qui est interdit par la loi, le contrôle des performances constitue une mesure autorisée et en général nécessaire dans le cadre d'un rapport de travail. Le contrôle des performances à l'aide de la technologie GPS se justifie généralement par les intérêts financiers tant de l'entreprise que de sa clientèle et, de l'avis du Tribunal fédéral tout comme du PFPD, est ainsi en principe autorisé. Il présuppose néanmoins l'information préalable des collaborateurs concernés (par ex. mention dans le contrat de travail).

Pourtant le profil des déplacements d'un véhicule équipé d'un GPS ne recouvre pas obligatoirement celui du collaborateur en service à l'extérieur. Ce dernier peut induire en erreur tant l'employeur que le client, notamment en laissant le véhicule au lieu de travail prescrit et en passant le temps de travail inscrit et facturé en partie dans un autre lieu. Pour cette raison, il est pour le moins douteux que la technologie GPS soit vraiment appropriée au contrôle des prestations. A notre avis, il existe des possibilités de contrôle plus efficaces; on pourrait par exemple demander aux clients de vérifier et de signer le rapport de travail du collaborateur. Si la technologie GPS est, dans un cas d'espèce, inappropriée en tant qu'instrument de contrôle des prestations, elle devient inutile et doit être jugée comme étant disproportionnée.

Lorsqu'il s'agit de déceler l'usage abusif du véhicule de service à des fins privées ou même de détecter rapidement son emplacement en cas de vol, le GPS est nécessaire car il ne peut être remplacé par une autre mesure. Là aussi, la prudence est de mise: le contrôle ciblé des abus privés de véhicules de service peut dans certains cas s'assimiler à un contrôle systématique du comportement. Comme nous l'avons établi plus haut, ce genre de contrôle n'est pas admis et ne doit en aucun cas servir de finalité dans le cadre de l'utilisation du GPS.

7 Economie et commerce

7.1 Contrôle du programme de fidélisation de la clientèle M-CUMULUS

Depuis le 1er novembre 1997, la Migros offre à sa clientèle un programme de fidélisation intitulé M-CUMULUS. En notre qualité d'autorité de surveillance en matière de protection des données, nous avons procédé à un contrôle des flux de données. Il est apparu que le traitement des données s'y déroule, dans l'ensemble, en conformité avec les principes de la protection des données. Mais malgré cette appréciation essentiellement positive, nous nous sommes aussi heurtés à des éléments qui devraient être modifiés du point de vue de la protection des données. Nous avons donc émis en tout deux recommandations et sept propositions de modification ou d'amélioration.

Une grande partie de la population suisse participe tous les jours au programme M-CUMULUS. A chaque achat, les clients reçoivent donc des points de bonus qu'ils peuvent ensuite utiliser comme de l'argent liquide dans les magasins Migros ainsi que dans diverses entreprises du groupe Migros. En contrepartie, ces clients autorisent la Migros à rassembler des informations détaillées sur leurs achats et à les exploiter à des fins de marketing. Sur la base de ces données d'achat, les participants au programme M-CUMULUS reçoivent ensuite des offres et des informations concrètes sur des produits Migros, à moins qu'ils n'y renoncent expressément. Le contrôle de protection des données que nous avons effectué était important non seulement en raison du grand nombre de participants à ce programme, mais aussi en raison du caractère sensible des données personnelles traitées.

Nous avons contrôlé en priorité les flux internes de données entre M-CUMULUS et les entreprises Migros (responsables du programme) ainsi que les flux de données entre la Migros et les partenaires du programme. Au préalable, nous nous sommes fait remettre les documents nécessaires et avons posé des questions. En février 2005, nous avons procédé à une analyse des faits sur place, dans les locaux de M-CUMULUS et de l'Infoline CUMULUS. Sur la base de la documentation remise et du contrôle effectué, nous sommes parvenus à une appréciation globale positive. Le traitement de données effectué dans le cadre de M-CUMULUS se déroule dans l'ensemble en conformité avec les prescriptions relatives à la protection des données. Nous avons toutefois émis deux recommandations conformément à l'art. 29 al. 3 LPD ainsi que sept propositions d'adaptation et d'amélioration.

Nos recommandations sont les suivantes:

- Le but des analyses du panier d'achat et de l'exploitation des données à des fins relevant du marketing doit être formulé de manière plus précise et plus transparente pour les clients dans les conditions générales;
- Il faut signaler, soit sur la brochure d'inscription, soit dans les conditions générales, les envois spéciaux qui sont effectués malgré la déclaration des clients selon laquelle ils renoncent à d'autres informations ou offres de Migros ou de ses entreprises partenaires doivent être signalés; ou alors de tels envois ne doivent plus être effectués à l'avenir.

Les propositions de modification et d'amélioration portaient essentiellement sur deux points: d'une part la reformulation des conditions générales, notamment concernant l'information sur le traitement des données, l'absence d'information quant au droit à être renseigné et du droit à la suppression des données, ainsi que la transmission de données à l'étranger. D'autre part, nous avons suggéré que le formulaire standard de suppression des données de M-CUMULUS indique clairement que seules les données personnelles sont supprimées, mais que les données d'achat collectées sont seulement anonymisées. Enfin, nous avons demandé que les clients soient mieux informés sur le délai de conservation effectif des données recueillies.

La Migros a tenu compte de nos deux recommandations et a effectué les adaptations nécessaires. Là où des divergences subsistaient, nous avons trouvé un consensus avec les responsables de M-CUMULUS.

Le rapport intégral de ce contrôle des flux de données a été publié, en langue allemande, sur notre site www.edsb.ch. Une annexe a été ajoutée au rapport final; celle-ci rend compte des avis et des réponses de la Migros au sujet du contrôle effectué au titre de la protection des données, ainsi que des réactions du PFPD.

7.2 Contrôle du programme de fidélisation de la clientèle Supercard

Depuis l'été 2000, Coop offre à sa clientèle la possibilité de participer à son programme de primes de fidélité Supercard. En notre qualité d'autorité de surveillance en matière de protection des données, nous avons contrôlé les flux de données générés par ce programme. Il est apparu que le traitement des données s'y déroule dans l'ensemble en conformité avec les principes de la protection des données. Mais, malgré cette appréciation essentiellement positive, nous nous sommes aussi heurtés à des éléments qui devraient être modifiés du point de vue de la protection des données. Nous avons donc émis en tout trois recommandations et six propositions de modification ou d'amélioration.

De très nombreuses personnes en Suisse participent chaque jour au programme Supercard. Chaque achat permet d'obtenir des points qui peuvent être ultérieurement échangés contre des primes. En contrepartie, Coop saisit les données de clients et les analyse à des fins de marketing et de statistiques. En participant au programme Supercard, le client donne son consentement à l'envoi, à son adresse personnelle, de publicité de la Coop ou de ses entreprises partenaires, à moins qu'il n'y renonce expressément. Ce contrôle était important tant en raison du grand nombre d'utilisateurs que du caractère sensible des données traitées.

Nous avons contrôlé en priorité les flux internes de données entre Coop Supercard et les entreprises du groupe Coop (responsables du programme) ainsi que les flux de données entre Coop Supercard et les partenaires du programme Supercard. Au préalable, nous nous sommes fait remettre les documents nécessaires et avons posé des questions. En février 2005, nous avons procédé à une analyse des faits sur place, dans les locaux de Coop Supercard.

Sur la base de la documentation remise et du contrôle effectué, nous sommes parvenus à une appréciation globale positive. Le traitement de données effectué dans le cadre de Supercard se déroule dans l'ensemble en conformité avec le droit de la protection des données. Nous avons toutefois émis trois recommandations conformément à l'art. 29 al. 3 LPD et six propositions d'adaptation et d'amélioration.

Nos recommandations sont les suivantes:

- Les personnes qui veulent s'inscrire au programme Supercard, que ce soit au moyen du bulletin d'inscription ou par Internet, doivent pouvoir consulter les conditions générales à cette occasion;
- Coop doit informer ses clients dans les conditions générales que l'utilisation de la Supercard permet d'établir la liste détaillée des achats effectués, qui est conservée pendant dix ans, le but de la conservation étant cependant strictement réglementé – les données récoltées ne pouvant pas, en particulier, être utilisées à des fins de marketing;
- Il faut soit faire ressortir plus clairement dans les conditions générales que les partenaires du programme peuvent enrichir les adresses dont ils disposent, soit renoncer complètement à l'enrichissement d'adresses.

Les propositions de modification et d'amélioration portaient sur plusieurs points essentiels: le consentement à l'envoi de publicité, la durée de conservation du talon d'inscription, l'indication claire des délais de conservation des données personnelles, ainsi que les mesures à prendre quant aux délais de conservation et de suppression des données personnelles auprès des partenaires du programme et, enfin, sur la consultation de la Superbox.

Coop a accepté les trois recommandations et a procédé aux adaptations requises. Là où des divergences subsistaient, nous avons trouvé un consensus avec les responsables de Coop Supercard.

Le rapport intégral de ce contrôle des flux de données a été publié, en langue allemande, sur notre site Internet www.edsb.ch. Une annexe a été ajoutée au rapport final; celle-ci rend compte des avis et des réponses de Coop concernant le contrôle effectué au titre de la protection des données, ainsi que des réactions du PFPD.

7.3 Consentement pour l'utilisation de données de clients à des fins publicitaires

L'utilisation de données personnelles pour des actions de marketing destinées aux propres clients d'une entreprise soulève constamment des questions et peut irriter les personnes concernées. Swisscom Fixnet a créé un formulaire permettant à ses clients de choisir par quels canaux de marketing les publicités peuvent leur être adressées.

Lorsqu'il existe déjà une relation commerciale entre une société et ses clients, la société peut, en l'absence d'une déclaration de volonté contraire de leur part, attirer l'attention de ses clients sur de nouvelles offres. Les clients ont cependant en tout temps le droit d'exiger expressément de ne plus recevoir de publicité.

Le fournisseur de services de télécommunications Swisscom Fixnet a créé l'an dernier un formulaire qui permet à ses clients de choisir s'ils souhaitent recevoir de la publicité par poste, par courriel, par téléphone ou par SMS. Par ailleurs, il est possible, dans le cadre d'Internet, de bloquer sur les sites web de Swisscom Fixnet et de Bluewin toute publicité axée sur les besoins spécifiques du client. De même, il est possible d'interdire les appels publicitaires pour des offres sur mesure. Finalement, il est également possible d'exiger que Swisscom Fixnet n'utilise pas à des fins de marketing l'information concernant la présélection d'un autre opérateur (Carrier Preselection).

Nous saluons le fait que les clients soient rendus attentif aux divers canaux de marketing et qu'ils puissent les bloquer à l'aide d'un formulaire détaillé rempli en fonction de leurs besoins. Les intérêts des clients seraient encore mieux servis si le formulaire était joint occasionnellement à la facture et s'il pouvait être téléchargé depuis Internet, plutôt que de devoir être commandé spécialement.

8 Finances

8.1 Activité de surveillance dans le domaine des cartes de crédit

Les clauses de consentement relatives au traitement des données figurant sur les demandes de cartes de crédit soulèvent régulièrement des questions et des critiques de la population. Nous avons donc examiné plus en détail les formulations correspondantes des principaux éditeurs de cartes et les avons évaluées en fonction du traitement des données qu'elles impliquaient. Nous parvenons à la conclusion que ces clauses apparaissent pires à la lecture qu'elles ne le sont en réalité. Dans le but d'augmenter la transparence dans ce domaine, nous avons décidé d'élaborer des clauses standard minimales et de les mettre à disposition des émetteurs de cartes de crédit.

Au cours des années 2003 et 2004, nous avons reçu de plus en plus de demandes de la population concernant les formulations dans les conditions générales de vente (CG) ou dans les demandes de cartes de crédit. La plupart des demandes concernaient les clauses dans lesquelles le requérant donne son accord pour des traitements de données décrits plus ou moins précisément (clauses de consentement). Diverses personnes concernées ont trouvé que les formulations allaient très loin et étaient trop peu transparentes.

Au début de l'année 2004, nous avons décidé d'examiner les clauses de consentement des principaux émetteurs de cartes. La vérification a porté, d'une part, sur la clarté et l'intelligibilité des formulations, respectivement sur la mesure dans laquelle celles-ci assuraient la transparence. D'autre part, il s'agissait naturellement aussi de se demander quels traitements les clauses de consentement examinées devaient couvrir.

La première appréciation – fondée uniquement sur l'étude des clauses de consentement – s'est avérée négative. En effet, les formulations examinées ne donnent pas une idée claire des traitements prévus. Néanmoins, avec certains émetteurs de cartes, nous avons réussi à améliorer des formulations qui seront incluses (ou ont déjà été incluses) dans la prochaine édition des conditions générales. A elles seules, ces améliorations ne suffisent cependant pas à revoir notre appréciation.

Il faut admettre que nous ne sommes pas en mesure d'étudier en détail tous les traitements de données qui sont effectués dans le système de paiement des cartes de crédit. La raison est que ce système est très complexe puisqu'il implique un grand nombre d'acteurs et d'éléments d'infrastructure et qu'il s'étend au monde entier.

C'est pourquoi nous nous sommes concentrés sur les traitements de données que les émetteurs de cartes effectuent d'une part lors de l'émission de la carte, d'autre part lors de l'utilisation de la carte. La conclusion la plus importante qui résulte de nos analyses concerne la quantité et le niveau de détail des données que les émetteurs de cartes reçoivent à chaque transaction. Nos recherches ont révélé que pour la plupart des transactions, les détails relatifs aux biens et aux prestations de services ne sont pas transmis aux émetteurs de cartes. Par conséquent, les émetteurs de cartes ne sont pas en mesure d'explorer ces données détaillées au moyen de techniques de Data Mining. Il s'est avéré que les émetteurs de cartes ne reçoivent que les informations qui figurent également sur la facture adressée au détenteur de la carte. Concrètement, cela signifie que pour chaque transaction, ils reçoivent, en plus des données relatives à la carte de crédit, un triplet de données composé de la date, du montant et du point de vente. Du point de vue de la protection des données, on peut constater que la communication de données du point de vente qui a accepté la carte de crédit vers les émetteurs de cartes est proportionnée puisque ces derniers ne reçoivent que les données dont ils ont besoin pour s'acquitter de leur tâche. Dès lors, nous considérons les traitements de données effectués par les émetteurs de cartes de crédit dont nous avons eu connaissance dans le cadre de nos recherches comme étant compatibles avec la protection des données.

D'autres traitements de données qui devraient être couverts par des clauses de consentement sont effectués auprès de deux types de destinataires de données. Il s'agit d'une part de prestataires de services externes qui fournissent des prestations informatiques pour le compte des émetteurs de cartes de crédit, mais qui ne poursuivent aucun objectif propre avec ces traitements de données. Sur la base des déclarations faites par les émetteurs de cartes – des entreprises proches des banques – nous partons du principe que les émetteurs de cartes exigent de la part de leurs partenaires externes qu'ils signent les accords de confidentialité contractuellement requis. Il s'agit d'autre part des entreprises partenaires qui coopèrent avec les émetteurs de cartes dans le cadre de certains programmes de fidélisation ou de promotion. Ainsi, dans le cas des programmes de fidélisation pour grands voyageurs, les émetteurs de cartes affirment qu'ils ne communiquent aux partenaires que le montant cumulé qui permet à son tour de calculer le nombre de milles-bonis. Etant donné que cette communication de données est limitée aux strict nécessaire, elle peut être considérée comme proportionnée.

En ce qui concerne les formulations dans les CG, nous avons déjà réussi, en collaboration avec les émetteurs de cartes, à réaliser certaines améliorations. Nous avons également examiné comment la transparence des CG pouvait être améliorée. Pour éviter de rendre les conditions générales encore plus compliquées, nous avons dé-

cidé de rédiger une clause minimale standard selon les règles suivantes: la clause de consentement doit tout d'abord être aussi concise que possible, elle doit ensuite être bien compréhensible pour les détenteurs de cartes, et finalement elle doit être complète. Pour pouvoir satisfaire à ces conditions, d'une part cette clause ne contient pas les éléments qui sont couverts par la loi, tels que le traitement effectué pour le compte d'un tiers (externalisation ou outsourcing). D'autre part, la clause est également épurée des éléments qui paraissent évidents. Nous allons soumettre cette clause - avec un rapport explicatif - aux émetteurs de carte, afin qu'ils puissent prendre position avant que nous la publiions.

8.2 Les sociétés de renseignement commercial et la protection des données

Le domaine du renseignement commercial est un des secteurs dans lesquels nous recevons chaque année un grand nombre de demandes. C'est pourquoi nous avons vérifié auprès de 4 grandes entreprises de ce secteur de quelle manière celles-ci respectaient les droits des personnes concernées en matière de protection des données.

S'agissant des traitements de données effectués par des entreprises actives dans le domaine du renseignement commercial, les personnes concernées s'adressent à nous pour plusieurs raisons. Soit elles sont étonnées voire même irritées d'apprendre qu'une entreprise traite des données les concernant, soit elles estiment que les données traitées par les entreprises en question sont inexactes.

Nous avons par conséquent décidé de vérifier auprès de quatre grandes entreprises de renseignement commercial de quelle manière celles-ci accordaient aux personnes concernées les droits d'accès, de rectification et d'effacement. Dans le cadre de notre examen des faits, nous avons envoyé une lettre à ces entreprises en les priant de nous fournir des documents sur la manière dont elles garantissent les droits des personnes concernées. Après avoir étudié la documentation reçue, nous avons également procédé à une visite de l'entreprise. Sur la base de l'analyse des informations reçues, nous rédigerons quatre rapports que nous transmettrons aux entreprises concernées. Ces rapports contiendront notre appréciation de la situation ainsi que - en fonction des résultats – des propositions d'amélioration ou des recommandations.

8.3 Communication de données personnelles relatives au trafic des paiements aux autorités américaines

La communication de données personnelles effectuée par Postfinance à un institut bancaire situé sur le territoire américain doit reposer sur un motif justificatif et la personne concernée doit être informée de manière appropriée. Suite à notre intervention, Postfinance a adapté sa pratique et proposé des mesures tenant compte de nos remarques.

Un client a donné l'ordre à Postfinance, par le biais de yellownet, de verser sur le compte d'une agence de voyages cubaine auprès d'une banque à Zürich une certaine somme en dollars américains. Le compte postal du client a été débité du montant en question, mais la société cubaine ne l'a pas reçu. Le client s'est adressé à Postfinance qui lui a répondu que son versement était bloqué par les autorités américaines en raison de l'embargo décidé à l'encontre de Cuba et que le montant se trouvait sur un compte du ministère des finances (U.S. Department of Treasury). Cette situation s'explique par le fait que les transactions en monnaies étrangères passent par un institut bancaire à l'étranger, dans le cas d'espèce un institut bancaire américain soumis à la législation américaine qui oblige cette banque à communiquer toutes les transactions financières touchant Cuba. Le client a indiqué à Postfinance que son versement concernait deux instituts financiers situés en Suisse (Postfinance et la banque à Zürich) et qu'il n'était indiqué nulle part sur le site «yellownet» que les transactions en monnaies étrangères à l'intérieur de la Suisse pourraient être effectuées via un Etat étranger.

Sur la demande de la personne concernée, nous avons analysé les traitements de données personnelles effectués par Postfinance dans le cadre de cette affaire. La loi fédérale sur la protection des données s'applique à la communication de données personnelles effectuée par Postfinance à la banque aux Etats-Unis. Par contre, les communications de données ultérieures effectuées par cette banque aux autorités américaines ne sont pas soumises à la législation suisse mais à la législation américaine. Postfinance n'est en droit de communiquer des données personnelles à la banque américaine qu'en présence d'un motif justificatif. Par motif justificatif, on entend le consentement de la personne concernée, un intérêt prépondérant public ou privé, ou une disposition légale. Dans le cas d'espèce, deux motifs justificatifs peuvent être envisagés: le consentement de la personne concernée ou un intérêt prépondérant privé. Pour être valable, le consentement doit toutefois être libre et éclairé. La personne concernée doit être ainsi clairement informée de la liste des données qui seront communiquées et du fait que celles-ci seront transmises dans un Etat qui ne dispose pas d'une législation sur la protection des données équivalente à la législation suisse.

Elle doit également être informée du fait que le destinataire des données pourrait être tenu de les livrer aux autorités en vertu de la législation de l'Etat en question. Outre le consentement de la personne concernée, Postfinance peut également faire valoir un intérêt prépondérant privé à communiquer à la banque les données nécessaires à l'exécution du contrat passé avec son client. L'exigence de transparence - qui découle du principe de la bonne foi - nécessite cependant une information appropriée, notamment dans le cas où la personnalité de la personne concernée devrait se trouver gravement menacée en raison de l'absence d'une protection des données équivalente à celle qui est garantie en Suisse. En l'occurrence, nous avons constaté que l'information n'était pas suffisante. De plus, pour les communications régulières vers un destinataire se trouvant dans un Etat ne disposant pas d'une législation équivalente, le fournisseur de données personnelles doit garantir, par le biais d'un contrat avec le destinataire, un niveau de protection des données équivalent à celui garanti par la législation suisse.

Sur la base des résultats de notre analyse, nous avons demandé à Postfinance d'informer les personnes concernées de manière appropriée et de garantir par le biais d'un contrat avec le destinataire que les données communiquées seront traitées d'une manière adéquate. En réponse à notre demande, Postfinance a proposé des mesures qui tiennent compte de nos remarques. Postfinance communique à la banque correspondante à l'étranger uniquement le montant de la transaction, le nom et le numéro de compte de la banque destinataire en Suisse ainsi qu'un numéro de référence. Postfinance, après avoir obtenu une procuration de la personne concernée, intervient auprès des autorités étrangères en cas de blocage d'une transaction. Afin d'informer les personnes concernées, Postfinance modifiera la clause de protection des données, dans le cadre des prochaines adaptations des conditions générales.

9. International

9.1 Union européenne

9.1.1 La mise en œuvre de l'accord d'association à Schengen

Les différents projets relatifs au système d'information Schengen de deuxième génération (SIS II) discutés au sein des comités et groupes de travail au niveau européen auront des effets sur les dispositions d'application en Suisse. Nous prenons position sur ces objets dans le cadre de la procédure de consultation des offices. Nous participons également aux séances du groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la Directive 95/46/CE et à celles de l'Autorité de contrôle commune du SIS.

La mise en oeuvre de l'accord d'association à Schengen a nécessité l'adaptation de plusieurs lois fédérales, en particulier le code pénal. Un certain nombre d'ordonnances doivent également être adaptées (par ex. ordonnance sur le système de recherches informatisées de police et ordonnance sur le système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police) tandis que d'autres doivent encore être élaborées (par ex. ordonnances relatives au SIS national et au bureau SIRENE).

La Suisse sera reliée dès 2008 au SIS II qui doit remplacer le système actuel. La Commission européenne a présenté un projet de règlement du Parlement européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du SIS II dans les domaines relevant du premier pilier (signalements de ressortissants de pays tiers aux fins de non-admission). La Commission européenne a aussi présenté un projet de décision du Conseil similaire pour les domaines relevant du troisième pilier (signalements de personnes recherchées aux fins d'arrestation et de remise ou aux fins d'extradition, signalements de personnes à des fins de protection ou de prévention de menaces, signalements de personnes recherchées dans le cadre de procédures judiciaires, signalements de personnes et d'objets aux fins de surveillance discrète ou de contrôle spécifique et signalements d'objets aux fins de saisie ou de preuves dans une procédure pénale). En matière de protection des données, il est prévu que les domaines relevant du premier pilier seront régis par la Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données tandis que les domaines rattachés

au troisième pilier seront soumis aux dispositions transposant la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (actuellement encore au stade de projet). Tous les projets susmentionnés sont actuellement traités par les différents comités et groupes de travail compétents pour le SIS II. Le résultat de ces travaux aura des effets sur les dispositions d'application en Suisse, notamment en matière de protection des données. Nous avons déjà pris position sur plusieurs de ces objets dans le cadre de la procédure de consultation des offices. Lorsque le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la Directive 95/46/CE traite de questions relatives à Schengen, le PFPD et un préposé cantonal à la protection des données représentent la Suisse en qualité d'observateurs. En tant qu'autorité de contrôle nationale indépendante en matière de protection des données, nous prenons aussi part aux travaux de l'Autorité de contrôle commune avec deux représentants (un membre de son secrétariat permanent et un représentant des préposés cantonaux à la protection des données).

9.1.2 Conférence européenne des commissaires à la protection des données

Les commissaires européens à la protection des données se sont réunis à Cracovie les 25 et 26 avril 2005 à l'invitation de l'Inspecteur général de la protection des données personnelles de la Pologne. Les commissaires ont adopté une déclaration encourageant l'adoption de dispositions légales régissant le traitement de données dans le cadre de la collaboration policière et judiciaire au sein de l'Union européenne. Les commissaires européens se sont également réunis à Montreux le 16 septembre 2005 et à Bruxelles le 24 janvier 2006. Lors de leur Conférence à Bruxelles, ils ont adopté un avis concernant le projet de décision-cadre du Conseil de l'Union européenne dans le domaine de la coopération policière et judiciaire.

Sous présidence polonaise, la conférence a réuni les commissaires à la protection des données des Etats membres de l'Union européenne et des autres pays européens ayant ratifié la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Ont également pris part aux travaux le contrôleur européen à la protection des données, des représentants de la commission européenne et du Conseil de l'Europe, ainsi que les autorités de contrôle communes d'Europol, Schengen et Eurojust.

Le thème principal de la conférence de Cracovie était le 10ème anniversaire 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 des personnes. Les commissaires ont ainsi eu l'occasion de dresser un premier bilan de l'application de la directive à la lumière des expériences nationales et de la jurisprudence de la Cour européenne de justice de Luxembourg. Ils ont également examiné l'influence de la directive sur le niveau de protection dans les pays de l'Union européenne et dans les pays tiers. A cette occasion, nous avons présenté les conséquences de la directive européenne pour la Suisse. Nous avons en particulier rappelé que la législation suisse est proche de la réglementation européenne et qu'elle se base également sur la Convention 108. A cet égard, la Suisse est au bénéfice d'une décision de la Commission européenne, datée du 26 juillet 2000, qui reconnaît le niveau de protection adéquat du droit suisse. Une première évaluation, effectuée en 2004, arrive à la conclusion que le système suisse de protection des données continue d'offrir un niveau de protection adéquat. De plus, nous avons souligné que la directive européenne influence le développement de notre droit interne et qu'elle sera transposée – certes de manière partielle – dans la législation sectorielle (conséquence des accords bilatéraux) ainsi que dans la loi générale de protection des données. En outre, nous avons relevé que les décisions de la Commission et les avis du Groupe de l'article 29 jouent également un rôle important dans la mise en œuvre de la protection des données en Suisse.

Les commissaires ont ensuite examiné les nouveaux instruments permettant le transfert de données personnelles à des pays tiers et en particulier les règles d'entreprise contraignantes. Ils ont débattu de l'importance de la sensibilisation et de l'éducation dans le domaine de la protection des données. Ils ont également échangé des informations et des expériences sur le recours à des conseillers à la protection des données au sein des entreprises et des organismes publics. L'institution de ces conseillers est jugée très positive par l'ensemble des pays qui la connaissent. Les commissaires ont en outre abordé certaines questions relatives à l'exercice du droit d'accès par les personnes concernées.

Enfin, les commissaires européens ont traité des problèmes de la protection des données au sein du 3ème pilier de l'Union européenne. Ils ont ainsi adopté un avis et une déclaration concernant l'échange d'informations dans le cadre de la poursuite pénale (http://www.edps.eu.int/legislation/05-04-26_krakow_pp_law_enforcement_EN.pdf). Tout en reconnaissant la nécessité des échanges d'informations entre les Etats pour lutter contre la criminalité et le terrorisme, les commissaires appellent à l'adoption d'une réglementation de protection des données pour le secteur de la coopération policière et judiciaire (3ème pilier). Cette réglementation ne doit pas seulement repren-

dre les principes définis dans la directive européenne, mais également établir de nouvelles règles qui prennent en considération le caractère particulier de la poursuite pénale. Les commissaires ont ainsi défini le cadre à prendre en compte lors de l'élaboration d'une telle réglementation.

Lors de leur Conférence à Bruxelles le 24 janvier 2006, les commissaires européens ont examiné le projet de décision-cadre du Conseil de l'Union européenne relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale et ont adopté un avis. Les commissaires ont salué l'adoption d'une décision-cadre régissant la protection des données dans le domaine de la coopération policière et judiciaire. Ils ont néanmoins proposé que le projet présenté par la Commission européenne soit amendé sur plusieurs points afin de renforcer la protection des données et d'assurer une meilleure cohérence entre les différents instruments existants. Les commissaires ont en particulier proposé que la décision ne se limite pas à l'échange de données personnelles mais qu'elle couvre l'ensemble des traitements de données personnelles dans le cadre du 3ème pilier, y compris la coopération judiciaire. Ils ont souligné qu'il devait y avoir une protection équivalente entre les données traitées en application de la directive 95/46 CE et celles couvertes par le 3ème pilier. Ce projet de décision-cadre fait partie de l'acquis de Schengen et, une fois adoptée, la décision s'appliquera également à la Suisse. Elle nécessitera des adaptations internes au niveau fédéral et cantonal. Il conviendra en particulier d'examiner l'opportunité de procéder à une harmonisation des règles nationales de protection des données. Dans ce contexte, il est souhaitable de transposer le droit européen dans la loi fédérale sur la protection des données.

9.2 Autres thèmes

9.2.1 Conférence internationale des commissaires à la protection des données

La 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée s'est tenue à Montreux du 14 au 16 septembre 2005. Organisée par le PFPD, elle réunissait les autorités de protection des données de quelque 40 Etats du monde entier. Elle s'est achevée avec l'adoption d'une déclaration finale visant au renforcement du caractère universel des principes de la protection des données. Les commissaires européens ont également adopté une résolution sur l'utilisation des données biométriques dans les passeports, les cartes d'identité et les documents de voyage ainsi qu'une résolution sur l'utilisation des données personnelles pour la communication politique.

A l'invitation du Préposé fédéral à la protection des données, la 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée s'est déroulée à Montreux du 14 au 16 septembre 2005. Organisée pour la première fois en Suisse, la Conférence a réuni quelque 350 participants provenant du monde entier. Sous le thème «Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités», les responsables des milieux économiques, scientifiques, politiques, ainsi que des représentants des organisations internationales gouvernementales et non gouvernementales ont débattu avec les commissaires à la protection des données de l'importance du droit à la protection des données dans le monde actuel. Tout au long des trois sessions plénières et des douze sessions parallèles (voir www.privacyconference2005.org, voir aussi *datum* 01/2005, www.edsb.ch), les conférenciers ont ainsi eu l'occasion d'aborder les différentes facettes du droit de la protection des données et la manière de rendre ce dernier plus effectif en tenant compte des enjeux politiques, socio-économiques et techniques. Les différents thèmes qui ont fait l'objet d'un débat sont en particulier les suivants: analyse des mécanismes juridiques et techniques mis en place pour protéger les personnes faisant l'objet d'un traitement de données personnelles, utilisation de données génétiques à des fins de recherche, défis de la lutte contre le terrorisme, rôle des entreprises privées dans l'accomplissement de tâches publiques, collaboration policière dans un Etat fédéral, apport des organisations internationales dans le respect du droit à la protection des données ou encore marketing politique. Les

participants à la Conférence se sont interrogés sur la pertinence des principes de la protection des données face à l'Internet et au développement des technologies invasives (RFID), sur l'effectivité de la surveillance en matière de protection des données et sur l'importance de l'auto-réglementation.

Plusieurs intervenants ont rappelé que la protection des données est un des éléments intangibles du fonctionnement d'une société démocratique moderne. Elle doit cependant faire face aux défis de la globalisation de nos sociétés et du développement des technologies de l'information. La technologie permet de traiter l'information rapidement ou en temps réel, de la collecter souvent à l'insu des personnes concernées, de la disséminer sans considération de frontières et de l'utiliser hors du contexte pour lequel elle avait été saisie. L'information peut être régie par différents systèmes juridiques de protection des données, voire échapper aux mécanismes de protection. Un même traitement peut faire l'objet de différentes procédures de notification ou de contrôle dans des Etats différents. Il peut être entravé du fait de règles trop restrictives ou de la mauvaise volonté de certains acteurs. Les personnes concernées ne pourront pas - ou difficilement - faire valoir leurs droits du fait de la dissémination des données en divers points du globe. Le contexte géopolitique actuel, la lutte contre le terrorisme, l'Internet, la biométrie, le développement des technologies invasives ou l'apparition des biobanques - sujettes à la convoitise de différents secteurs d'activités - renforcent l'importance de la défense des droits et des libertés fondamentales lors du traitement de données personnelles. On perçoit cependant un risque d'affaiblissement de la protection des données due à une certaine banalisation du concept de vie privée et à une relativisation des exigences de la protection des données. Ce risque est aussi la conséquence d'une trop grande différence entre les systèmes juridiques existants ou d'une trop grande dispersion et multiplication des dispositions de protection des données.

On constate également un déséquilibre dans la pesée des intérêts en présence qui se fait au détriment de la protection des droits et des libertés fondamentales. Or une société démocratique ne peut fonctionner que si l'Etat et les personnes privées se voient imposer des limites dans le traitement des données personnelles. Il existe un intérêt public à ce que les Etats assurent une protection suffisante des données indépendamment d'une requête des personnes concernées. Comme l'a relevé le Professeur Bertil Cottier, face à l'augmentation considérable des échanges internationaux et à la mobilité croissante des personnes, des services et des biens, la protection des données ne peut - à l'instar de tout autre domaine du droit - éviter une certaine unification. Une simplification et une harmonisation des règles et des procédures existantes sont nécessaires. Il s'agit aussi de développer des instruments qui garantissent le respect des droits des citoyens et citoyennes du monde entier, tout en permettant aux organismes

publics et privés d'effectuer leurs tâches légitimes: utilisation de nouvelles technologies garantissant le respect de la vie privée, encouragement de l'auto-réglementation et programmes de sensibilisation et d'éducation à la protection des données.

Forts de ces constats et donnant suite à une initiative du PFPD, les commissaires à la protection des données ont adopté à l'unanimité une déclaration finale (voir annexe 11.2). L'objectif de la déclaration de Montreux est de promouvoir la reconnaissance du caractère universel des principes de protection des données. Convaincus que le droit à la protection des données et à la vie privée est une condition indispensable dans une société démocratique pour garantir le respect des droits des personnes, la libre circulation des informations et une économie de marché ouverte, qu'il s'agit d'un droit fondamental des personnes et qu'il est nécessaire d'en renforcer le caractère universel, les commissaires appellent au développement d'une convention universelle de protection des données. A cette fin, ils s'engagent à collaborer avec les gouvernements et les organisations internationales et supranationales. Les commissaires appellent en particulier:

- l'ONU, à préparer un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée en tant que droits de l'homme exécutoires;
- l'ensemble des gouvernements du monde, à favoriser l'adoption d'instruments juridiques de protection des données et de respect de la vie privée conformes aux principes de base pour la protection des données et de les étendre à leurs relations mutuelles;
- le Conseil de l'Europe, à inviter les Etats non membres du Conseil de l'Europe qui ont une législation de protection des données à adhérer à la Convention et à son protocole additionnel;
- les chefs d'Etat et de gouvernement présents au Sommet mondial de l'Information à Tunis, à inclure dans leur déclaration finale un engagement à développer ou renforcer le cadre juridique destiné à assurer le droit à la protection de la vie privée et des données personnelles:
- les organisations internationales et supranationales, à s'engager à se conformer aux règles de protection des données;
- les organisations internationales non gouvernementales, à élaborer des standards de protection des données;
- les fabricants de matériel informatique et de logiciel, à développer des produits et des systèmes intégrant des technologies respectueuses de la vie privée.

La déclaration a également pour objectif de renforcer la collaboration entre les différentes autorités de protection des données, ainsi que la collaboration entre ces autorités et les différents acteurs concernés par le traitement de données personnelles. La réalisation des objectifs de la déclaration devra régulièrement faire l'objet d'une évaluation. La première évaluation interviendra lors de la 28ème Conférence internationale.

Les commissaires ont en outre adopté une résolution présentée par l'Allemagne concernant l'utilisation de la biométrie dans les passeports, les cartes d'identité et les documents de voyage. Ils y soulignent que l'utilisation de la biométrie aura un impact considérable sur la société et devrait être précédée d'un débat ouvert et universel. Les commissaires demandent que des garanties efficaces soient mises en place pour limiter d'emblée les risques inhérents à la nature de la biométrie (voir annexe 11.3).

Les commissaires, enfin, ont adopté une résolution présentée par l'Italie concernant l'utilisation de données personnelles pour la communication politique. Tout en rappelant l'importance de la communication politique dans le processus démocratique, les commissaires soulignent que toute activité de communication politique impliquant le traitement de données personnelles doit respecter les libertés et les droits fondamentaux des personnes concernées, y compris le droit à la protection des données. Ces traitements doivent être conformes aux principes de protection des données, en particulier les principes de minimisation, de licéité et de la bonne foi, de la proportionnalité, de la finalité, de l'exactitude et de la transparence (voir annexe 11.4).

Les textes des résolutions sont disponibles sur le site www.privacyconference2005.org.

10 Le Préposé fédéral à la protection des données

10.1 Les publications du PFPD – Nouvelles parutions

Notre attention a été attirée à plusieurs reprises sur le risque que peuvent présenter, pour la protection des données, les pixels espions (Webbugs). Nous avons analysé les pixels espions inclus d'une part dans les pages Internet, et d'autre part dans les bulletins d'information personnalisés acheminés par courriel. Des sociétés recourant à ces techniques nous ont fourni des informations que nous avons complétées par nos propres investigations sur Internet.

Les résultats de notre analyse sont publiés dans l'annexe 11.6 du présent rapport ainsi que sur notre site web www.edsb.ch.

10.2 Une nouvelle formule pour la newsletter du PFPD

En décembre 2005, après plus de deux ans d'interruption, nous avons fait paraître la newsletter *datum* dans sa nouvelle formule. *datum* paraîtra désormais deux fois par an et s'adresse à un large public intéressé par les questions de protection des données, sans qu'il soit nécessairement spécialiste en la matière.

C'est en mars 2003 que nous avons publié notre dernière newsletter. Durant l'année écoulée, nous avons réexaminé notre concept et y avons apporté quelques modifications avant la reparution. L'objectif de notre publication est de porter les préoccupations de la protection des données devant un large public et de sensibiliser la population à la protection de ses propres données.

En effet, en tant que citoyenne ou citoyen, nous sommes tous les jours confrontés à des questions de protection des données. Et cela pas uniquement en raison du nombre croissant de caméras vidéos qui surveillent les places, les moyens de transport public, les halls de gare et les magasins. L'évolution extrêmement rapide des technologies de la communication tout comme les lois antiterroristes - qui, dans les pays occidentaux, gagnent toujours plus de terrain - mettent en danger les droits fondamentaux de la personnalité. Parallèlement, la prise de conscience qu'il faut protéger nos données et notre personnalité est diversement développée.

datum contiendra d'une part des informations sur des sujets touchant directement les citoyennes et les citoyens en matière de protection des données, abordera des questions d'intérêt général. D'autre part, nous donnerons des conseils concrets devant permettre de protéger ses données au quotidien. En effet, chacun d'entre nous peut

et doit, dans la vie de tous les jours, mettre un tant soit peu en pratique les principes de la protection de données: lorsque nous surfons sur Internet, lorsque nous communiquons notre adresse électronique, lorsque nous donnons des informations sur notre personne, que ce soit dans un magasin ou en participant à un concours, ou encore lorsque nous utilisons la technologie sans fil bluetooth sur notre téléphone portable ou les fonctions wireless-lan de notre ordinateur portable.

La rubrique «Thèmes» est l'occasion de consacrer de longs articles à des sujets tout aussi actuels qu'importants. Les autres rubriques présentent les derniers développements en matière de protection des donnés dans le domaine technique et informatique («En bref»), d'intéressants articles ou coupures de presse dans «Lu dans la presse», et enfin des «Conseils» utiles à un respect quotidien de la protection des données. La rubrique «Agenda» signale les dates importantes figurant à l'agenda du PFPD et «Mise à jour» donne les nouveautés que l'on peut trouver sur le site du PFPD.

datum paraîtra en principe deux fois par an, en mars et en octobre. Il peut être consulté sur le site web du PFPD à la rubrique Publications/Newsletter et imprimé en format pdf. Les personnes s'inscrivant sur la liste d'envoi du PFPD (www.edsb.ch) seront en outre averties de la parution de nouvelles publications sur notre site web. Il est prévu que le prochain numéro de datum paraisse en octobre 2006.

10.3 Saisie et consultation en ligne des fichiers annoncés auprès du PFPD.

La nouvelle application Web pour la gestion et la consultation du registre des fichiers annoncés auprès du PFPD est en phase de réalisation. Un formulaire d'annonce simplifié et trilingue permettra aux organes fédéraux de gérer leurs annonces électroniquement et de manière autonome. Après validation par le PFPD, ces dernières seront mises à disposition du public par le biais d'un module de recherche et d'impression accessible depuis notre site web.

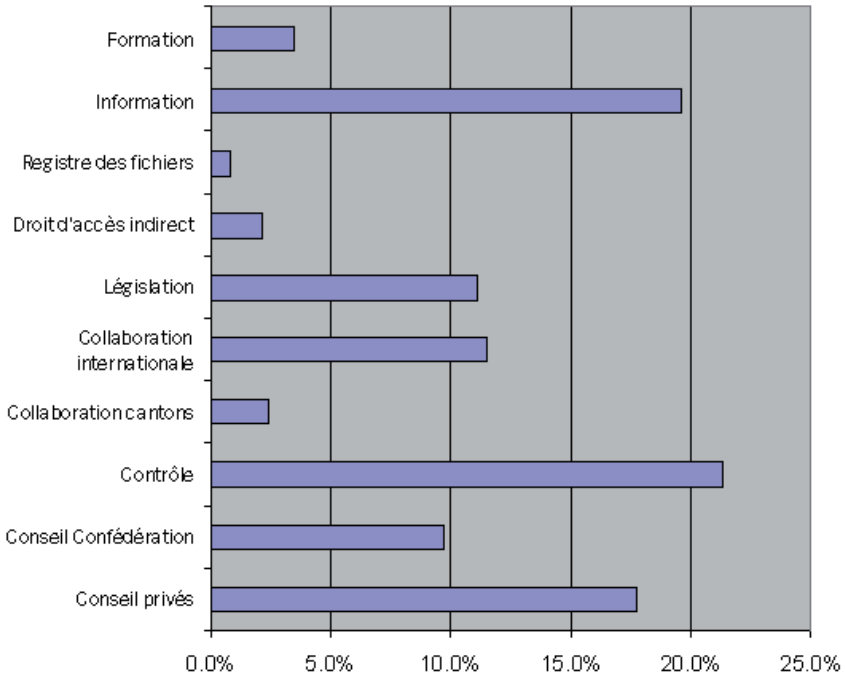
Selon la loi, le PFPD est tenu de gérer et de mettre à disposition du public un registre des fichiers soumis à déclaration. Actuellement, les formulaires d'annonce sont remplis manuellement; les informations sont ensuite saisies par nos soins dans une base de données locale avant d'être publiées dans des cahiers subdivisés par départements pour l'administration fédérale et par domaines d'activité pour les personnes privées. Les opérations de saisie se sont cependant révélées fastidieuses et les cahiers difficiles à maintenir à jour. De plus, le projet de révision de la LPD requiert la tenue d'un registre des fichiers accessible en ligne (nouvel article 11a). Il était donc temps de réviser le mode d'annonce des fichiers et de consultation du registre.

Un appel d'offres a été lancé pour la création d'un nouveau programme. Le cahier des charges contenait notamment les exigences suivantes: la reprise intégrale des données existantes, le support complet des trois langues nationales officielles, un formulaire de saisie en ligne des fichiers (navigateur Web) par les différents organes fédéraux responsables, la validation et la mise en ligne des annonces par le PFPD, et un masque public de recherche multicritère permettant la visualisation et l'impression des données relatives aux fichiers en question. Dans le délai prescrit, nous avons reçu plusieurs offres satisfaisant à tout ou partie de ces exigences. Le partenaire offrant le meilleur rapport qualité/prix a ensuite été choisi pour la réalisation de ce nouveau programme.

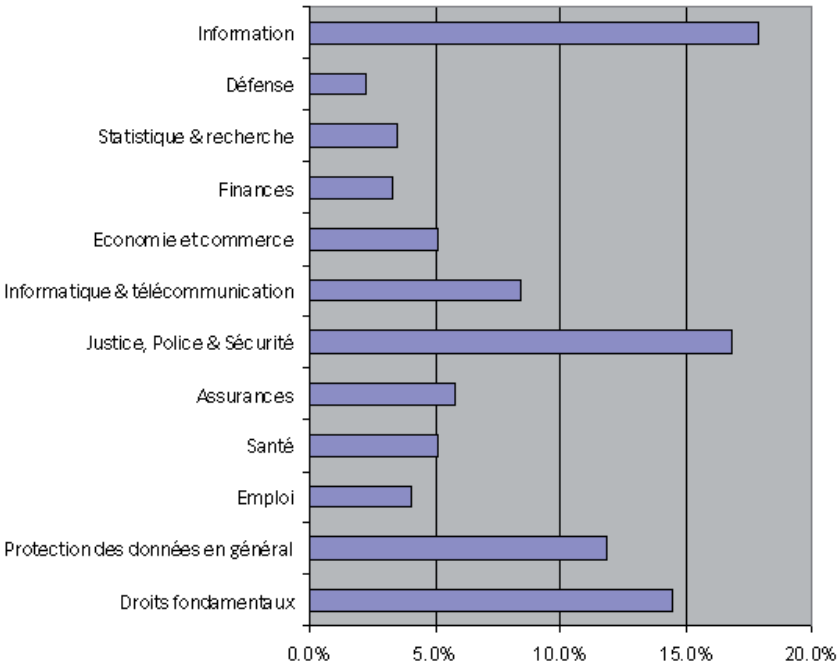
Après réception et prise en main du nouveau programme, nous commencerons par le mettre à disposition des organes fédéraux responsables de l'annonce des fichiers et de leur mise à jour (le plus souvent les conseillers à la protection des données des offices) et nous fournirons de nouveaux formulaires trilingues simplifiés aux personnes privées. Ces dernières pourraient également disposer, à terme, d'une solution d'annonce en ligne. Après une période de consolidation des données existantes et de correction des éventuelles erreurs de jeunesse du nouveau programme, nous pourrons finalement offrir au public la possibilité de consulter en ligne - de manière facile et conviviale - le registre des fichiers. Les différentes fonctionnalités de ce nouveau service seront peu à peu intégrées dans notre site www.edsb.ch.

10.4 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2005 au 31 mars 2006

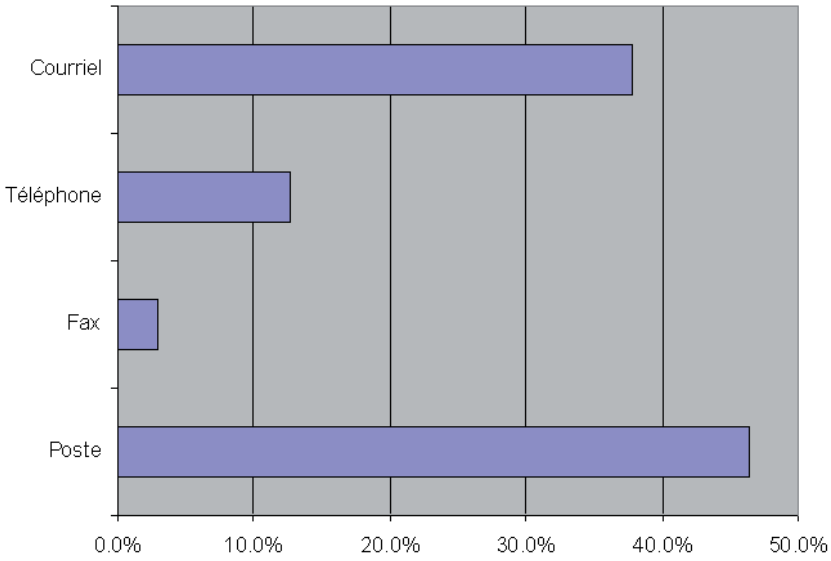
Charge de travail par tâches



Charge de travail par domaine



Provenance des demandes



10.5 Secrétariat du Préposé fédéral à la protection des données

Préposé fédéral à la protection des données:	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:	10 personnes
Chancellerie:	3 personnes

11 Annexes

11.1 Contrat-type pour l'externalisation du traitement de données à l'étranger

Voir paragraphe 11.1 de la partie en langue allemande.

11.2 Déclaration de Montreux

«Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités»

Les Commissaires à la protection des données et à la vie privée réunis à Montreux lors de leur 27e Conférence internationale (14 au 16 septembre 2005) ont convenu de promouvoir la reconnaissance du caractère universel des principes de protection des données et ont adopté la déclaration finale suivante:

1. Donnant suite à la déclaration adoptée à Venise lors de la 22e Conférence internationale des commissaires à la protection des données et à la vie privée,
2. Rappelant la résolution sur la protection des données et les organisations internationales adoptée à Sydney lors de la 25e Conférence internationale des commissaires à la protection des données et à la vie privée,
3. Constatant que le développement de la société d'information est dominé par la globalisation des échanges d'information, le recours à des technologies de plus en plus invasives de traitement des données et l'augmentation des mesures sécuritaires,
4. Préoccupés par les risques croissants d'une surveillance omniprésente des individus dans le monde entier,
5. Relevant les avantages et risques potentiels des nouvelles technologies de l'information,
6. Préoccupés par les disparités encore existantes entre les systèmes juridiques de différentes parties du monde et notamment de l'absence de garantie de protection des données dans certains endroits, laquelle sape une protection des données effective et globale,

7. Conscients que l'augmentation rapide des connaissances dans le domaine de la génétique peut faire de l'ADN des êtres humains la donnée personnelle la plus sensible; conscients également que cette accélération dans les connaissances rend plus important d'assurer au niveau légal une protection adéquate de ces données,

8. Rappelant que la collecte de données à caractère personnel et leur traitement ultérieur doivent être effectués dans le respect des exigences de la protection des données et de la vie privée,

9. Reconnaissant la nécessité dans une société démocratique de lutter efficacement contre le terrorisme et le crime organisé, mais rappelant que cet objectif peut mieux être atteint si les droits de l'homme et notamment la dignité humaine sont respectés,

10. Convaincus que le droit à la protection des données et à la vie privée est une condition indispensable dans une société démocratique pour garantir le respect des droits des personnes, la libre circulation des informations et une économie de marché ouverte,

11. Convaincus que le droit à la protection des données et à la vie privée est un droit fondamental des personnes,

12. Convaincus qu'il est nécessaire de renforcer le caractère universel de ce droit afin d'obtenir une reconnaissance universelle des principes régissant le traitement de données à caractère personnel tout en respectant les diversités juridiques, politiques, économiques et culturelles,

13. Convaincus de la nécessité d'assurer à l'ensemble des citoyens et citoyennes du monde des droits individuels sans discrimination lors du traitement de données à caractère personnel les concernant,

14. Rappelant que dans sa déclaration de principes et son plan d'action, le Sommet mondial sur la société de l'information (Genève 2003) a souligné l'importance de la protection des données et de la vie privée pour le développement de la société de l'information,

15. Rappelant que le groupe international de travail sur la protection des données dans le domaine des télécommunications recommande de prendre en compte dans le cadre d'accords multilatéraux le décalogue de protection de la vie privée qu'il a élaboré en 2000 [1],

[1] http://www.datenschutz-berlin.de/doc/int/iwgdpt/tc_en.htm

16. Reconnaissant que les principes de protection des données découlent d'instruments juridiques internationaux contraignants ou non contraignants, notamment les Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, les Principes directeurs des Nations Unies pour la réglementation des fichiers informatisés contenant des données à caractère personnel, la Directive européenne 95/46 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et les principes directeurs de vie privée de la Coopération économique Asie-Pacifique (APEC),

17. Rappelant que ces principes sont en particulier les suivants:

    - Principe de licéité et de loyauté de la collecte et du traitement des données,
    - Principe d'exactitude,
    - Principe de finalité,
    - Principe de proportionnalité,
    - Principe de transparence,
    - Principe de participation individuelle et notamment la garantie du droit d'accès des personnes concernées,
    - Principe de non-discrimination,
    - Principe de sécurité,
    - Principe de responsabilité,
    - Principes d'une surveillance indépendante et de sanctions légales,
    - Principe du niveau adéquat de protection lors de flux transfrontières de données.

Compte tenu de ce qui précède,

Les Commissaires à la protection des données et à la vie privée manifestent leur volonté de renforcer le caractère universel de ces principes. Ils conviennent de collaborer en particulier avec les gouvernements et les organisations internationales et supra nationales au développement d'une convention universelle pour la protection des personnes à l'égard du traitement des données personnelles.

A cet effet, les Commissaires appellent

a. L'Organisation des Nations Unies à préparer un instrument juridique contraignant énonçant en détail le droit à la protection des données et à la vie privée en tant que droits de l'homme exécutoires;

b. l'ensemble des gouvernements du monde de favoriser l'adoption d'instruments juridiques de protection des données et de respect de la vie privée conformes aux principes de base pour la protection des données, et de l'étendre à leur relations mutuelles;

c. le Conseil de l'Europe, conformément à l'article 23 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, à inviter les Etats non membres du Conseil de l'Europe qui ont une législation de protection des données, à adhérer à la Convention et à son protocole additionnel;

En plus, les Commissaires encouragent

les Chefs d'Etat et de gouvernement qui se réunissent à Tunis pour le sommet mondial de l'information (16-18 novembre 2005) à inclure dans leur déclaration finale un engagement à développer ou renforcer le cadre juridique destiné à assurer le droit à la protection de la vie privée et des données personnelles de tous les citoyens dans le cadre de la société de l'information en accord avec l'engagement pris au Sommet de Santa Cruz par les Chefs d'Etat et de gouvernement ibéro-américains (novembre 2003) et avec celui pris au Sommet de Ouagadougou par les Chefs d'Etat et de gouvernement des Etats ayant le français en partage (novembre 2004).

Les Commissaires appellent également

a. Les organisations internationales et supra nationales à s'engager à se conformer à des principes compatibles avec les principaux instruments internationaux qui touchent à la protection des données et à la vie privée, et en particulier de mettre en place des autorités de surveillance agissant de manière indépendante et dotées de pouvoirs de contrôle;

b. Les organisations internationales non gouvernementales, telles que les associations économique et commerciale ou les associations de consommateurs à élaborer des standards fondés sur les principes de base de la protection des données ou conformes à ces principes;

c. Les fabricants de matériel informatique et de logiciel à développer des produits et des systèmes intégrant des technologies respectueuses de la vie privée.

Les Commissaires conviennent en outre

a. de renforcer notamment l'échange d'informations, la coordination de leurs activités de surveillance, le développement de standards communs, la promotion de l'information sur les activités et les résolutions de la Conférence;

b. de promouvoir la coopération avec les Etats qui ne se sont pas encore dotés d'autorités de surveillance de la protection des données indépendantes;

c. de promouvoir l'échange d'informations avec les organisations internationales non gouvernementales actives dans le domaine de la protection des données et de la vie privée;

d. de collaborer avec les conseillers à la protection des données d'organisations;

e. de créer un site web permanent en particulier comme base commune d'information et de gestion des ressources.

Les Commissaires à la protection des données et à la vie privée conviennent de procéder régulièrement à l'examen de la réalisation des objectifs de la présente déclaration. La première évaluation se fera lors de la 28e Conférence internationale en 2006.

11.3 Résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage

27ème Conférence internationale des Commissaires à la protection des données et à la vie privée,

Montreux 16 septembre 2005

La 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée adopte la résolution suivante:

Constatant que les gouvernements et les organisations internationales, notamment l'Organisation de l'aviation civile internationale (OACI), sont en train de mettre au point des règles et des normes techniques en vue de l'insertion de données biométriques (empreintes digitales, reconnaissance faciale) dans les passeports et documents de voyage aux fins de lutter contre le terrorisme et d'accélérer les contrôles aux frontières et les procédures d'enregistrement («check-in»);

Consciente du fait que le secteur privé traite aussi de plus en plus de données biométriques, le plus souvent sur une base volontaire;

Tenant compte du fait que les données biométriques peuvent être collectées à l'insu de la personne concernée, car elle peut laisser inconsciemment des traces biométriques;

Rappelant que la biométrie rendra le corps humain "lisible par la machine" et que les informations biométriques pourraient être utilisées en tant qu'identificateur unique universel;

Soulignant que l'utilisation à large échelle de la biométrie aura un impact considérable sur la société tout entière et devrait par conséquent faire l'objet d'un débat ouvert au niveau mondial,

la Conférence demande:

1. l'application, à un stade précoce, de garanties efficaces en vue de limiter les risques inhérents à la nature de la biométrie,

2. une distinction stricte entre les données biométriques collectées et conservées à des fins publiques (p. ex. contrôles aux frontières) sur la base d'obligations légales, et celles qui sont collectées à des fins contractuelles sur la base du consentement,

3. la limitation, par des mesures techniques, de l'utilisation des données biométriques dans les passeports et les cartes d'identité à des fins de vérification, par comparaison des données figurant dans le document avec celles fournies par son titulaire lorsqu'il le présente.

11.4 Résolution sur l'utilisation de données personnelles pour la communication politique

Montreux (Suisse), du 14 au 16 septembre 2005

La Conférence,

Considérant que la communication politique est un instrument fondamental de la participation des citoyens, des forces politiques et des candidats à la vie démocratique et reconnaissant l'importance de la liberté du discours politique en tant que droit fondamental;

Considérant que la citoyenneté présuppose que les citoyens ont le droit d'obtenir des informations et d'être informés de façon adéquate durant les campagnes électorales politiques et administratives; considérant que ces droits s'appliquent également à d'autres sujets, événements et opinions politiques utiles pour faire des choix, en connaissance de cause, dans d'autres domaines de la vie politique - votations, choix des candidats, accès à l'information au sein d'organisations politiques ou émanant de représentants élus;

Considérant que les forces politiques et les organisations politiques en général, ainsi que les représentants élus, utilisent différentes stratégies de communication et de levée de fonds, sources d'information et nouvelles technologies dans le but d'établir des contacts directs et personnalisés avec de vastes catégories de personnes concernées;

Considérant que, dans un nombre croissant de pays, on constate une tendance à l'augmentation de la communication institutionnelle de la part des candidats et organes élus, y compris au niveau local ou par le biais de la cyberadministration; considérant que cette réalité, qui nécessite parfois le traitement de données personnelles, est conforme au droit des citoyens à être informés de l'activité des élus susmentionnés;

Considérant que, dans ce cadre, une grande quantité de données personnelles sont continuellement collectées par des organisations politiques et sont parfois traitées selon des méthodes agressives qui impliquent diverses techniques comprenant des sondages, la collecte d'adresses électroniques par des logiciels/moteurs de recherche, des techniques de démarchage politique à l'échelle d'une ville tout entière ou des formes de décisions politiques prises à l'aide de la télévision interactive et de fichiers servant à isoler les votants ; considérant que ces données comprennent parfois de

manière illicite, des données sensibles touchant aux activités ou convictions morales et politiques réelles ou supposées ou aux choix électoraux (en plus des adresses électroniques, numéros de téléphone, comptes de messagerie et informations en rapport avec des activités professionnelles et des relations familiales);

Considérant qu'il est ainsi établi de manière intrusive le profil de diverses personnes qui sont couramment classées – parfois de façon inexacte ou sur la base d'un contact superficiel – dans la catégorie des sympathisants, des partisans, des adhérents ou des membres d'un parti, afin de renforcer la communication personnalisée avec certains groupes de citoyens;

Considérant que ces activités doivent se dérouler dans un cadre légal et correct;

Considérant qu'il est nécessaire de protéger les libertés et les droits fondamentaux des personnes concernées et de prévenir, par des mesures appropriées, les ingérences injustifiées, les atteintes et les coûts dont elles pourraient être victimes, notamment les incidences négatives et les discriminations potentielles dans leur sphère privée ainsi que l'abandon, de leur part, de certaines formes de participation politique;

Considérant qu'il serait possible d'atteindre l'objectif de la protection tout en prenant en compte, dans chaque cas, les intérêts du public liés à certaines activités de communication politique de même que les modalités et garanties adéquates s'agissant des communications internes destinées à des membres d'un parti ou à de simples citoyens;

Considérant que, dans cette perspective, le marketing responsable peut être encouragé sans qu'on restreigne pour autant la circulation des idées et des propositions politiques et que - bien que la communication politique présente parfois un caractère promotionnel - il a certaines particularités qui le distinguent du marketing commercial;

Considérant que dans plusieurs juridictions, la législation de la protection des données est déjà applicable à la communication politique;

Considérant qu'il est nécessaire de garantir le respect des principes régissant la protection des données et de créer, à l'échelle mondiale, une norme minimale susceptible de contribuer à l'harmonisation des niveaux de protection des personnes concernées, en se fondant notamment sur des codes de conduite nationaux et internationaux et en prenant en compte des solutions et des règles spécifiques en vigueur dans divers pays;

Considérant que les Commissaires à la protection des données et à la vie privée pourraient jouer un rôle croissant en planifiant des actions coordonnées, notamment aussi en coopération avec d'autres autorités de surveillance compétentes dans les domaines des télécommunications, de l'information, des sondages d'opinion et des activités électorales;

Adopte la résolution suivante:

Toute activité de communication politique - y compris celles qui ne se rapportent pas aux campagnes électorales - qui implique le traitement de données personnelles devrait respecter les libertés et les droits fondamentaux des personnes concernées, y inclus le droit à la protection des données personnelles, et devrait être conforme aux principes de protection des données reconnus, en particulier:

Principe de minimisation

Les données personnelles ne devraient être traitées que lorsque cela s'avère nécessaire pour atteindre les buts dans lesquels elles ont été spécifiquement collectées.

Principe de licéité et de loyauté de la collecte

Les données personnelles devraient être collectées d'une manière licite sur la base de sources reconnaissables et traitées loyalement. Il conviendrait de s'assurer que, conformément à la loi, les sources sont accessibles au public ou ne peuvent être utilisées que dans certains buts spécifiques, selon certaines modalités ou pour une occasion ou un laps de temps limités.

Une attention spécifique devrait être accordée si des méthodes agressives sont utilisées pour entrer en contact avec les personnes concernées.

Principe de la qualité des données

Les autres principes régissant la qualité des données devraient être respectés durant le traitement de ces dernières. Les données devraient notamment être exactes et pertinentes, non excessives et tenues à jour en rapport avec les buts spécifiques dans lesquels elles ont été collectées, tout particulièrement lorsque l'information se réfère aux opinions sociales ou politiques ou aux convictions éthiques d'une personne concernée.

Principe de la finalité

Les données personnelles issues de sources d'information, d'institutions ou d'associations privées ou publiques peuvent être utilisées pour la communication politique si leur traitement ultérieur est compatible avec les buts dans lesquels elles ont été collectées et qui ont déjà été portés à la connaissance des personnes concer-

nées, notamment lorsque les données sont sensibles. Les représentants élus doivent respecter ces principes lorsqu'ils utilisent, pour la communication politique, des données personnelles collectées pour l'exercice de leurs fonctions institutionnelles.

Les données personnelles collectées initialement pour des activités de marketing sur la base du consentement éclairé peuvent être utilisées si le but de la communication politique est spécifiquement mentionné dans la déclaration de consentement.

Principe de la proportionnalité

Les données personnelles ne devraient être traitées que selon des modalités et des procédés conformes aux buts visés, notamment lorsque les données se réfèrent à des électeurs potentiels ou lorsqu'elles sont comparées avec des données extraites d'archives ou de banques de données différentes.

Les données personnelles, tout particulièrement celles qui sont conservées après l'événement pour lequel elles ont été collectées, peuvent être traitées ultérieurement si les buts de la communication politique sont en voie de réalisation.

Principe de l'information des personnes concernées

Une notice d'information conforme aux moyens de communication choisis sera fournie aux destinataires avant toute collecte de données; elle spécifiera l'identité du responsable de traitement (candidats, directeur de campagne externe; groupe local de partisans ou associations locales ou déléguées, parti dans sa globalité, etc.) et la nature des flux de données auxquels il faut s'attendre entre ces entités.

La personne concernée devrait être informée lorsque les données ne sont pas obtenues par son entremise, et au moins lorsqu'elles ne sont pas conservées uniquement à titre temporaire.

Principe du consentement

Il conviendrait de s'assurer que le traitement des données personnelles se fonde sur le consentement de la personne concernée ou repose sur un autre motif légitime prévu par la loi. Le traitement des données devrait respecter les règles spécifiques de chaque pays en fonction des sources ou des moyens de communication utilisés, notamment dans le cas d'adresses électroniques, de numéros de fax, de SMS ou d'autres messages multimédias et d'appels téléphoniques préenregistrés.

Principe régissant la conservation des données et mesures de sécurité

Tout responsable de traitement – qu'il s'agisse d'une force politique ou d'un candidat– doit prendre toutes les mesures de sécurité techniques et organisationnelles pour sauvegarder l'intégrité des informations collectées et pour prévenir toute perte et/ou utilisation abusive par des personnes ou entités non autorisées.

Droits des personnes concernées

Les personnes concernées devraient avoir le droit d'accéder à leurs données, d'en obtenir la rectification, de les faire bloquer et/ou effacer, de s'opposer à des communications non désirées et de demander – gratuitement et au moyen de procédés simples – à ne plus recevoir de nouveaux messages. Ces droits devraient être mentionnés dans les informations qui leur sont destinées.

Des mesures et des sanctions adéquates devraient être prévues pour le cas où ces droits seraient bafoués.

11.5 Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Voir paragraphe 11.5 de la partie en langue allemande.

11.6 Explications relatives aux webbugs (pixels espions) et aux bulletins d'information personnalisés

En 2004, l'attention du Préposé fédéral à la protection des données (PFPD) a été attirée sur le risque que peuvent présenter, pour la protection des données, les pixels espions (Webbugs). Nous avons analysé les pixels espions inclus d'une part dans les pages Internet, et d'autre part dans les bulletins d'information personnalisés acheminés par courriel. Des sociétés recourant à ces techniques nous ont fourni des informations que nous avons complétées par nos propres investigations sur Internet. Le présent document explique ce que sont les pixels espions, le risque qu'ils présentent pour la protection des données et les moyens de les maîtriser.

Pixels espions dans les pages Internet

Les pixels espions sont utilisés dans le Web à diverses fins, par exemple pour mesurer et attester le taux de fréquentation d'un site. L'exploitant peut ainsi prouver l'impact de son offre, ce qui est particulièrement important dans le domaine publicitaire. Des compteurs simples, qui enregistrent sur une page Web le nombre de visiteurs, recourent également à cette technologie.

Les pixels espions dans les pages Internet sont des images transparentes comportant un seul pixel. Ils permettent de connaître:

- l'adresse IP utilisée (et ainsi la localisation approximative de l'internaute) ;
- la date, l'heure et la durée de la visite;
- des caractéristiques techniques telles le système d'exploitation, le type de navigateur et la résolution de l'écran;
- les pages consultées antérieurement (referer URL).

Les pixels espions sont implantés par le propriétaire du site. Concrètement, une société X souhaite connaître la fréquentation de son site; elle s'adresse à la société Y qui lui fournit un pixel espion à placer sur son propre site. Y peut mesurer de la sorte aussi bien le nombre des visiteurs que leurs mouvements sur le Web. Les adresses IP sont toutefois gérées de manière dynamique, c'est-à-dire que l'internaute en reçoit une nouvelle à chaque accès à son fournisseur. Pour déterminer si c'est bien le même visiteur qui consulte un site Web, un témoin (cookie) est souvent envoyé à son ordinateur – il s'agit d'un petit fichier texte qui permet l'identification et qui sera lu lors des visites ultérieures.

Si la société Y, pour reprendre l'exemple précédent, utilisait des pixels espions sur plusieurs pages Web, elle obtiendrait des informations au sujet de toutes ces pages visitées par l'internaute lors d'une session (donc avec la même adresse IP).

Normalement, les données précitées ne permettent pas d'identifier le visiteur d'une page Internet. Seul le fournisseur d'accès sait lesquels de ses clients utilisent à un moment donné telle ou telle adresse IP. Soumis au secret des télécommunications, il ne peut communiquer les données personnelles de ses clients à des tiers.

L'utilisateur s'identifie toutefois lui-même lorsqu'il remplit un formulaire Web. Par exemple, il commande un produit et fournit son nom, son adresse et éventuellement d'autres données. En recourant parallèlement à des témoins, il serait possible de déterminer aussi les pages consultées par l'internaute lors d'autres sessions antérieures et les adresses IP de cet utilisateur.

Les personnes qui consultent des pages Web ne savent généralement pas qu'elles comportent des pixels espions et ignorent le traitement réservé aux données.

Une autre question a trait au maître du fichier: si des données sont traitées par un tiers, par exemple la société Y, il convient de déterminer qui, du mandant (X) ou du mandataire (Y) est maître du fichier au regard de la loi sur la protection des données. En principe, il s'agit de celui qui traite effectivement les données. Si le rôle du mandataire se borne à fournir l'infrastructure technique permettant le traitement d'une quantité prédéfinie de données, le mandant reste maître du fichier. En revanche, si le mandataire traite de son propre chef des données, en assurant par exemple le marketing du mandant, il est responsable de ce traitement et a de ce fait qualité de maître du fichier. Cela vaut tout particulièrement lorsque le mandataire œuvre pour le compte de plusieurs mandants et qu'il traite les données de visiteurs fréquentant les sites de plusieurs de ces mandants. Il devient alors possible d'établir des profils de personnalité en observant le comportement de l'internaute dans plusieurs sites. Ces profils ont une haute valeur commerciale, et une utilisation abusive ne peut pas être exclue.

Exigences à l'égard des fournisseurs de services Internet (société X et société Y)

- La page Internet consultée doit indiquer que l'adresse IP, l'heure de la visite, les spécifications techniques, les déplacements et les URL des pages précédemment consultées sont visibles non seulement pour le propriétaire de la page visitée, mais également pour un tiers;
- des mesures techniques et organisationnelles doivent empêcher l'exploitation, par un mandataire, du comportement d'un internaute visitant les sites de plusieurs mandants;
- lorsque des formulaires invitent à fournir des données personnelles, une technologie appropriée doit permettre d'isoler l'adresse IP de l'internaute des données personnelles transmises;
- les données d'un internaute (notamment l'adresse IP) obtenues par des pixels espions ne doivent être conservées que le temps strictement nécessaire au but pour lequel elles ont été collectées (par ex. la mesure du taux de fréquentation d'un site Web), à l'issue duquel elles doivent être détruites ou anonymisées pour empêcher tout rapprochement avec une personne existante;
- dans la mesure du possible, on ne devrait pas associer des pixels espions et des témoins. Dans le cas contraire, l'internaute doit être clairement informée de l'existence et des risques de cette combinaison;
- le maître du fichier doit garantir en tout temps le droit d'accès prévu dans la loi sur la protection des données (LPD).

Conseils aux utilisateurs

- Le texte source de la page Web vous permet de repérer des pixels espions, tout comme des logiciels spécifiques
  (par ex. Bugnosis, http://www.bugnosis.org);
- effacez régulièrement les témoins de votre ordinateur;
- lisez attentivement les considérations relatives à la protection des données, et ne visitez une page que si vous êtes d'accord avec les dispositions prises;
- en cas de doute, interrogez les fournisseurs ou faites valoir le droit d'accès que vous confère la loi sur la protection des données.

Pixels espions dans les bulletins d'information personnalisés

Outre les pages Web, les messages électroniques peuvent également contenir des pixels espions : ils servent alors à vérifier si et quand le message est ouvert, et quels liens sont activés.

Une société peut elle-même envoyer à ses clients (potentiels) puis gérer des bulletins d'information électroniques. Il existe toutefois des fournisseurs spécialisés qui offrent à leurs clients une large palette de prestations dans le domaine de l'adressage et de la gestion de lettres d'information électroniques. Les destinataires s'abonnant eux-mêmes à ces bulletins, on parle de « permission marketing » (en d'autres termes de démarchage avec l'autorisation du destinataire). Un tel mandataire recrute probablement ses clients dans les branches les plus diverses (banques, agences de voyage, commerce automobile, etc.).

Qu'est-ce qu'un bulletin d'information personnalisé?

Lorsqu'il souscrit un abonnement à un bulletin d'information électronique, le destinataire fournit son adresse de messagerie et, éventuellement, d'autres données telles son nom, son adresse ou ses centres d'intérêt. En insérant des pixels espions dans ces bulletins, le fournisseur peut savoir si, quand et combien de fois son message a été ouvert par le destinataire, pour autant que le message ait été envoyé en format HTML et que le destinataire se trouve en ligne. L'adresse IP permet d'autres constats, par exemple de savoir si le bulletin a été ouvert au travail ou à domicile. Mais on peut aussi apprendre sur quels liens le destinataire a cliqué, en les munissant d'un code spécifique à chaque adresse destinataire. La distribution des bulletins suivants peut alors être individualisée parce que l'on pourra choisir les thèmes auxquels l'abonné s'est précédemment intéressé dans sa navigation ou renoncer à évoquer des produits qu'il a ignorés.

Aspects liés à la protection des données

Le fournisseur peut donc cerner les centres d'intérêt du destinataire en fonction de ses réactions au bulletin d'information. Les précisions sur le délai et le lieu d'ouverture du courrier permettent de déterminer le comportement de la personne concernée, et il est difficile de dire dans quelle mesure cette dernière est au courant de cela. Un fournisseur travaillant pour de nombreux mandants de branches économiques très diverses pourrait a priori analyser en profondeur les centres d'intérêt d'une personne donnée, et parvenir – comme le permettent les pixels espions des pages Web – à établir des profils de personnalité d'une extrême précision. Nous n'avons toutefois pas trouvé d'exemple de tels agissements.

Exigences à l'égard des fournisseurs

- Quiconque offre un bulletin d'information électronique doit informer l'abonné, en toute transparence, du traitement auquel les données seront soumises;
- les personnes concernées doivent notamment savoir si le bulletin d'information est géré par un tiers : en effet, si elle est abonné à plusieurs bulletins, ces derniers pourraient être techniquement gérés par le même fournisseur;
- des mesures techniques et organisationnelles doivent empêcher qu'un fournisseur exploite les données personnelles d'un même abonné collectées sous couvert de plusieurs sociétés clientes;
- le maître du fichier doit garantir en tout temps le droit d'accès prévu dans la loi sur la protection des données.

Conseils aux utilisateurs

- Avant de souscrire un abonnement à un bulletin d'information, lisez attentivement les considérations relatives à la protection des données;
- en cas de doute, interrogez les fournisseurs et faites valoir le cas échéant le droit d'accès que vous confère la loi sur la protection des données. Au besoin, déposez une plainte civile.