16ème Rapport d'activités 2008/2009

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2008/2009 du Préposé fédéral à la protection des données et à la transparence

Le Préposé fédéral à la protection des données et à la transparence est tenu de fournir périodiquement au Conseil fédéral un rapport sur son activité (article 30 de la loi fédérale sur la protection des données).
Le présent rapport couvre la période du 1er avril 2008 au 31 mars 2009.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.016.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

Ténacité et pragmatisme: les deux maîtres-mots d'une véritable protection des données

Facebook et les autres sites de réseautage social sur Internet rencontrent un succès croissant. Leurs utilisateurs se comptent aujourd'hui par millions. Les jeunes surtout trouvent très «cool» de se faire des «amis» par voie électronique et d'échanger nouvelles et impressions, étalant ainsi au grand jour des aspects très personnels de leur vie. Mais les moins jeunes ne sont pas en reste et utilisent de plus en plus ce qui est devenu un véritable instrument de mobilisation: en effet, les acteurs de la vie politique ont compris que les plateformes de réseautage social permettaient d'atteindre de nombreux électeurs par effet de boule de neige, et ce presque gratuitement. Ainsi, il semblerait que le nouveau président des Etats-Unis Barack Obama doive son élection à l'utilisation des médias sociaux durant sa campagne électorale. En Suisse aussi, les politiques ont découvert le réseautage social. Le référendum contre les passeports biométriques est le premier ayant abouti grâce à Internet. Aujourd'hui, la Toile est une source d'informations toujours plus riche que de très nombreux acteurs de la société, de l'employeur aux services secrets, mettent à profit au service de leurs intérêts.

Au cours de l'année écoulée, les multiples aspects de ce nouveau phénomène nous ont fortement occupés. Quel impact ont-ils en termes de protection des données? Que nous le voulions ou non, nul ne peut plus freiner l'expansion du réseautage social en ligne. Pour nous, il s'agit en premier lieu d'observer avec vigilance cette évolution afin de détecter à temps les abus manifestes et de pouvoir intervenir. Parallèlement, nous concentrons nos efforts sur un point précis: la diffusion, sur notre site web, de directives de comportement préconisant une utilisation sans danger de ce très récent instrument de communication. Pour que nous puissions accomplir notre devoir d'information avec efficacité, nous devons certes faire preuve de bon sens, mais avons aussi besoin du soutien des autres acteurs sociaux. Je pense en premier lieu aux écoles.

Ténacité et pragmatisme sont deux qualités indispensables dans un domaine très délicat de la collecte et du traitement des informations par les autorités, à savoir la protection de l'Etat. Depuis des années, nous demandons que le droit d'accès indirect soit transformé en droit direct et que la protection juridique des citoyens soit améliorée. Tout juste vingt ans après l'affaire des fiches, le sujet refait son apparition. A l'origine, la révélation du fichage de députés bâlois d'origine kurde. Cette nouvelle

affaire a suscité un tel sentiment d'insécurité que les demandes de consultation des documents officiels qui nous sont parvenues ont décuplé. En application de l'art. 18 al. 3 LMSI, nous avons informé à titre exceptionnel les personnes qui en avaient fait la demande si elles étaient fichées ou non. Pour nous a été déterminant le fait que ces personnes pouvaient craindre d'être fichées en raison de leurs activités politiques, ce qui est incompatible avec l'art. 3 LMSI. Au début de l'année sous revue, nous avions déjà fait usage à quatre reprises de cette disposition d'exception. Dans ce contexte, nous avions examiné avec grande attention la question de savoir si la pratique suivie par le SAP était compatible avec les limites posées par l'art. 3 LMSI. Selon cet article, les informations relatives à l'engagement politique ou à l'exercice de la liberté d'opinion, d'association et de réunion ne peuvent pas être traitées. Une fois de plus, ces cas ont souligné les lacunes du droit d'accès indirect qui ne permet pas un véritable examen des données consignées dans les fichiers.

A la lumière de ces faits, la conseillère nationale Susanne Leutenegger Oberholzer a déposé une intervention parlementaire demandant qu'un droit direct d'accès aux données soit aussi garanti dans le domaine de la protection de l'Etat si les intérêts de la protection de l'Etat ne s'y opposent pas. Le Conseil fédéral a accepté sa proposition. La révision actuellement en cours de la LMSI touche encore une autre de nos anciennes requêtes: après le refus initial du Conseil national d'entrer en matière sur cette révision en raison de ce qui était considéré comme un durcissement discutable de la loi, il apparaît clairement après la décision de renvoi du Conseil des états que le Conseil fédéral doit améliorer avant tout la protection juridique.

Au cours de la première moitié de l'année écoulée, le Conseil fédéral a accepté l'évaluation de la mise en œuvre des dispositions de Schengen et a pris les décisions requises en vue d'améliorer l'indépendance du PFPDT et d'augmenter les ressources. Rien n'entravait donc plus la mise en œuvre de l'accord de Schengen. Nous nous sommes depuis attelés aux tâches de contrôle et de surveillance qui nous incombent. L'ambassade de Kiev a tout d'abord été au programme. Un autre contrôle a été effectué en collaboration avec les autorités de protection des données des Etats Schengen. Cette année, nous nous occuperons de l'Office fédéral de la police et d'autres ambassades. La collaboration requise avec les cantons a démarré et sera menée à bien sur la base d'un règlement mis en place par le PFPDT.

Pour ce qui est des projets associant la santé et les nouvelles technologies (ce que l'on appelle désormais «eHealth» ou «e-santé»), le Conseil fédéral a accéléré le rythme. Ce n'est plus qu'une question de temps: le dossier médical électronique du patient deviendra bientôt réalité. Mais le chemin pour y parvenir sera encore jalonné de nombreux obstacles, surtout dans le domaine de la protection des données. Nous suivons

ce projet de près car si les préoccupations de la protection des données ne sont pas suffisamment prises en compte, les risques pour les citoyens pourraient être graves. A nos yeux, une chose est claire: pour les patients, l'introduction du dossier électronique doit constituer une amélioration de la protection des données médicales par rapport au dossier papier traditionnel.

La loi sur la transparence est entrée dans sa troisième année. L'évaluation requise par la loi au terme de trois ans a été établie par l'IDHEAP (Institut de hautes études en administration publique). Ses conclusions, dans leur majorité, ne nous ont pas surpris: les ressources affectées aux procédures de médiation et à la formulation de recommandations, telles que les prévoit cette loi, demeurent insuffisantes. Nous ne pouvons pas tenir les délais légaux prévus et les autres tâches qui nous ont été déléguées ne peuvent pas être menées à bien correctement. Par voie de conséquence, la loi sur la transparence demeure très peu connue du public et, toujours selon cette étude, le nombre des demandes de consultation des documents officiels en proportion de la population est, en Suisse, de loin le plus bas par rapport à d'autres pays. Du point de vue conceptuel, une lacune considérable a été identifiée: si l'administration ne suit pas nos recommandations et que, pour des raisons financières, le requérant ne porte pas le cas devant le Tribunal administratif fédéral, il n'existe plus de possibilité de règlement devant les juges, surtout dans les situations politiquement délicates. L'étude recommande donc que nos prérogatives soient renforcées: dans les cas importants, la LPD devrait nous octroyer le droit de porter nous-mêmes l'affaire devant l'instance la plus élevée. Nous sommes curieux de voir comment les responsables politiques réagiront face à ces recommandations. Leur réaction sera pour nous un point de repère quant à la priorité que les responsables politiques donnent à la mise en œuvre de la loi sur la transparence. Là aussi, nous demeurerons vigilants et nous ferons montre de ténacité tout comme de pragmatisme dans l'optique d'une véritable application de la loi sur la transparence.

Hanspeter Thür

Répertoire des abréviations

ACC	Autorité de contrôle commune (Schengen)
AEIP	autorité indépendante d'examen des plaintes en matière de radiotélévision
AFAPDP	Association francophone des Autorités de protection des données personnelles
AFIS	Système automatique d'identification des empreintes digitales
ASMS	Association suisse des spécialistes en recherches de marché et sociales
CODIS	Combined DNA Index System
COMAI	Centre d'observation médicale de l'assurance-invalidité
COMCO	Commission de la concurrence
CSA	Corps suisse d'aide humanitaire
DDC	Direction du développement et de la coopération
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
fedpol	Office fédéral de la police
GEWA	Système de traitement des données en matière de lutte contre le blanchiment d'argent
IPAS	Système informatisé de gestion et d'indexation de dossiers et de personnes de l'office fédéral de la police
ISA	Système d'information relatif aux documents d'identité
IWGDPT	International Working Group on Data Protection in Telecommunications
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAA	Loi fédérale sur l'assurance-accidents
LAGH	Loi fédérale sur l'analyse génétique humaine

LAMal	Loi fédérale sur l'assurance-maladie
LBA	Loi fédérale sur le blanchiment d'argent
LCA	Loi fédérale sur le contrat d'assurance
LIFD	Loi fédérale sur l'impôt fédéral direct
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOGA	Loi sur l'organisation du gouvernement et de l'administration
LP	Loi fédérale sur la poursuite pour dettes et la faillite
LPD	Loi fédérale sur la protection des données
LPD	Loi fédérale sur la protection des données
LPers	Loi sur le personnel de la Confédération
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité
LRTV	Loi fédérale sur la radio et la télévision
LSF	Loi sur la statistique fédérale
LSIP	Loi fédérale sur les systèmes d'information de police de la Confédération
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
OCPD	Ordonnance sur les certifications en matière de protection des données
OFAS	Office fédéral des assurances sociales
OFCOM	Office fédéral de la communication
OFEV	Office fédéral de l'environnement
OFIT	Office fédéral de l'informatique et de la télécommunication
OFJ	Office fédéral de la justice
OFPER	Office fédéral du personnel
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique

OPP 3	Ordonnance sur les déductions admises fiscalement pour les cotisations versées à des formes reconnues de prévoyance
OSRPP	Ordonnance sur les exceptions à l'obligation de garder le secret dans la prévoyance professionnelle et sur l'obligation de renseigner incombant aux organes de l'AVS/AI
PA	Loi fédérale sur la procédure administrative
PFPDT	Préposé fédéral à la protection des données et à la transparence
RFA	Régie fédérale des alcools
SAP	Service d'analyse et de prévention (DDPS)
SAS	Service d'accréditation suisse
SECO	Secrétariat d'Etat à l'économie
sedex	secure data exchange
SER	Secrétariat d'Etat à l'éducation et à la recherche
SGPD	Système de gestion de protection des données
SGSI	Système de gestion de sécurité de l'information
SIS	Système d'information de Schengen
SMR	Service médical régional
SSMC	Société suisse des médecins-conseils et médecins d'assurances
TAF	Tribunal administratif fédéral
UID	Numéro d'identification des entreprises
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Certification de produits/systèmes en matière de protection des données

Nous avons reçu le mandat d'édicter dans les meilleurs délais les directives fixant les critères spécifiques qu'un produit doit remplir dans le cadre d'une certification. Or, cette tâche s'avère particulièrement difficile, étant donné qu'une certification ISO 15408 étendue à la protection des données est intrinsèquement complexe, en partie déphasée par rapport à notre situation législative et surtout difficile à mettre sur pied. Pour ce qui concerne les services de la technologie de l'information (services TI), la norme ISO 20000 se prêterait a priori assez bien, mais le législateur ne semble pas avoir voulu couvrir ce domaine. Finalement, il y a bien le catalogue de critères EuroPriSe, mais ce dernier forme un amalgame assez hardi entre produits et services, et ressemble plus à une liste de questions portant sur des produits ou services et leurs exploitants, et n'est en outre guère adapté au droit suisse.

Après avoir édicté avec succès les directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir (voir «directives sur la certification de l'organisation et de la procédure» sur notre site web www.leprepose.ch sous la rubrique Thèmes - protection des données - certification), le PFPDT est tenu d'édicter d'ici au 1er janvier 2010 les directives fixant les critères spécifiques qu'un produit doit remplir dans le cadre d'une certification. Cette tâche s'annonce particulièrement ardue pour les raisons suivantes:

L'univers des produits/systèmes est très différent de celui de l'organisation, comme en témoigne la certification «tierce partie» basée sur la norme ISO/IEC 15408:2005 (critères d'évaluation pour la sécurité TI, aussi connue sous l'appellation anglaise «Common Criteria for Information Technology Evaluations»). Cette norme correspond à la version 2.3 des critères communs, dont la révision majeure de 2006 a donné l'actuelle version CC 3.1. Fondée sur la norme associée ISO/IEC 18045:2005 (Méthodologie pour l'évaluation de la sécurité TI, aussi connue sous l'appellation anglaise «Common Methodology for Information Technology Evaluations»), l'évaluation des produits est tout d'abord effectuée par un laboratoire indépendant au bénéfice d'une accréditation SAS. Le rapport d'évaluation est ensuite transmis à l'organisme gouvernemental

de certification de produits (qui n'existe pas encore en Suisse) pour appréciation et éventuel octroi du certificat, dont la reconnaissance est assurée au niveau européen par l'accord SOG-IS (Senior Officials Group for Information Security) et au niveau international par l'accord CCRA (Common Criteria – Recognition Arrangement). Hormis la différence structurelle constatée, il faut encore relever que la certification ISO 15408-1/3 est relativement complexe, donc plutôt onéreuse, et porte sur la sécurité intrinsèque et non sur la protection des données et qu'elle comporte beaucoup d'exigences extrinsèques aux produits/systèmes. L'extension de cette norme à la protection des données ne nous paraît ainsi pas du tout facile à appréhender.

Par ailleurs, les produits/systèmes TI n'incluent pas foncièrement les services TI, pour lesquels la norme ISO/IEC 20000:2005 (Information Technology – Service Management) pourrait servir de référence. Une extension de la sécurité à la protection des données serait ici aisément envisageable, tout comme nous l'avons fait pour l'extension des Systèmes de gestion de sécurité de l'information (SGSI, ISO 27001) aux SGPD (cf. notre rapport d'activités 2007/2008, ch. 1.1.2). Cependant, il ne ressort pas clairement de la LPD et de l'Ordonnance sur les certifications en matière de protection des données (OCPD), ni de leurs commentaires, que le législateur a voulu couvrir les services dans le cadre de la certification de produits et systèmes. L'édiction de directives pour les services TI nous paraît dès lors prématurée.

Enfin, nous avons également examiné la grille d'évaluation élaborée par le Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein, aujourd'hui reprise comme «EuroPriSe Criteria Catalogue V0.3». Ce projet de «sceau européen de protection des données» vise à certifier que les produits ou services TI facilitent une utilisation conforme aux régulations européennes et à la législation des pays pilotes (Agence de Protection des Données de la Communauté de Madrid et Commission Nationale Informatique et Libertés). De notre point de vue, le catalogue de critères proposé, introduit de manière assez hardie par les services TI, ne bénéficie apparemment pas d'un très large soutien européen et ressemble davantage à une «checklist» portant sur des caractéristiques du produit ou service et sur des exigences par rapport à leurs exploitants, qu'à un catalogue d'exigences pour produits certifiables; en outre, il nécessiterait une adaptation assez conséquente au droit suisse. Nous allons donc poursuivre nos investigations dans ce vaste domaine, afin d'édicter les directives attendues dans les meilleurs délais.

1.1.2 Entrée en vigueur des directives pour la certification des systèmes de gestion de la protection des données

Nos directives sur les exigences minimales envers un système de gestion de la protection des données ainsi que leurs annexes sont entrées en vigueur le 1er septembre 2008. Ces directives s'appuient fortement sur les normes internationales ISO 27001 et ISO 27002, l'accent ayant cependant été déplacé de la sécurité des informations à la protection des données.

Comme décrit dans notre 15e rapport d'activités 2007/2008 (ch. 1.1.1), l'ordonnance sur les certifications en matière de protection des données (OCPD) prévoit que le PFPDT émet des directives concernant les exigences minimales envers un système de gestion de la protection des données. Ces directives relatives à la certification de l'organisation et des procédures (désignées par la suite par «directives SGPD») ont maintenant été élaborées. Elles sont entrées en vigueur le 1er septembre 2008.

Nos directives SGPD s'appuient fortement sur les normes et les standards internationaux, en particulier sur ISO 27001:2005 (en ce qui concerne le système de gestion de la sécurité de l'information), mais également sur ISO 9001:2000 (en ce qui concerne le système de gestion), tel que cela est prévu dans l'OCPD. Lors de l'élaboration de nos directives, nous avons surtout repris dans les normes ISO précitées les exigences envers les systèmes de gestion. En même temps, nous avons constaté que l'accent avait été mis sur les points qui concernent la protection des données. Ainsi, nous avons remplacé la notion de «sécurité de l'information», contenue dans ISO 27001:2005, par celle de «protection des données». De plus, l'analyse des risques selon ISO a été complétée par l'introduction d'une analyse de (non-)conformité. Quant aux objectifs et aux mesures, les directives mentionnent les principes généraux selon la LPD. Ces objectifs et mesures ont été concrétisés dans notre «Code de bonne pratique pour la gestion de la protection des données». Ce code de bonne pratique décrit pour chaque principe de la protection des données l'objectif à atteindre, la mesure à prendre ainsi que son application subséquente (une description plus détaillée se trouve dans notre 15e rapport d'activités 2007/2008, ch. 1.1.2).

Maintenant que nos directives SGPD sont entrées en vigueur, toute entreprise privée est libre de se faire accréditer auprès de l'organisme suisse d'accréditation (SAS) afin de pouvoir procéder à des certifications en matière de protection des données.

1.1.3 Recensement 2010

Dans le cadre des travaux préparatoires en vue du recensement fédéral de la population 2010, nous avons collaboré avec l'Office fédéral de la statistique et pris position sur les projets de modification de l'ordonnance sur le recensement fédéral de la population et de l'ordonnance concernant l'exécution de relevés statistiques fédéraux.

En 2010, le recensement fédéral de la population sera réalisé pour la première fois en Suisse principalement sur la base d'informations provenant des registres administratifs ainsi que partiellement sur des enquêtes par sondage auprès d'échantillons de ménages. Lors des travaux préparatoires relatifs à ce recensement, nous avons collaboré avec l'Office fédéral de la statistique et pris position dans le cadre des procédures de consultation relatives au projet de modification de l'ordonnance sur le recensement fédéral de la population et au projet d'ordonnance concernant l'exécution de relevés statistiques fédéraux. A cette occasion, nous avons en particulier souligné la nécessité, d'une part, de définir un niveau minimal de sécurité pour les transferts électroniques de données personnelles qui ne sont pas réalisés par le biais de la plateforme Sedex et, d'autre part, de préciser les modalités d'anonymisation des données personnelles dans le cadre du recensement fédéral de la population 2010.

1.1.4 Numéro d'identification des entreprises

Après une première version du projet prévoyant la création de la base légale pour le nouveau numéro d'identification des entreprises (UID) dans une ordonnance et suite à nos critiques, l'Office fédéral de la statistique a accepté d'élaborer une nouvelle loi. L'utilisation de l'UID dans le secteur Business to Business reste cependant à notre avis problématique.

L'Office fédéral de la statistique (OFS) envisage l'introduction d'un numéro d'identification des entreprises (UID, abréviation de «Unternehmens-Identifikationsnummer»). Le but de ce projet est de faciliter les échanges d'informations à l'intérieur de l'administration (Governement to Governement, G2G), entre les entreprises et l'administration (Business to Governement, B2G) ainsi que entre les différentes entreprises (Business to Business, B2B).

Dans une première version du projet, l'OFS prévoyait d'introduire la base légale dans l'Ordonnance sur le Registre des entreprises et des établissements. Suite à nos critiques à ce sujet (voir notre 15e rapport d'activité, ch. 1.1.6), l'OFS a reconnu la nécessité

d'élaborer une base légale au sens formel et nous a soumis un projet de loi sur le numéro d'identification des entreprises et le registre d'identification des entreprises (Loi UID).

Nous avons pu trouver des solutions de compromis sur différents points portant en particulier sur la sécurité des données et leur communication à des tiers. Toutefois une divergence demeure concernant l'utilisation de l'UID entre différentes entreprises (secteur B2B): il s'avère en effet qu'une telle utilisation augmente fortement les possibilités de surveillance et d'atteintes à la personnalité. Les risques relatifs aux applications possibles dans le secteur B2B, tels que le profilage, n'ont été ni analysés ni même relevés dans la documentation présentée. Nous sommes d'avis que l'utilisation de l'UID pour les applications B2B devrait être interdite, ou à tout le moins limitée.

1.1.5 Nouvel accord entre la Suisse et les États-Unis sur la communication des données de passagers d'avion

Un nouvel accord a été conclu entre la Suisse et les États-Unis sur la communication par les compagnies aériennes des données de passagers aux autorités américaines. Dans notre prise de position, nous avons critiqué le fait que le nouvel accord ne comporte plus sa propre clause de protection des données, mais renvoie simplement au droit américain.

La Suisse et les États-Unis ont réglementé la communication de données personnelles des passagers aux autorités américaines par les compagnies aériennes dans un accord de 2005 (cf. notre 13e rapport d'activités 2005/2006, ch. 1.1.2). Ce dernier est arrivé à échéance en 2008, raison pour laquelle un nouvel accord a été conclu.

Le nouvel accord stipule que les données personnelles à communiquer sont, en termes de protection des données, soumises à la «System of Records Notice (SORN) for the Automated Targeting System (ATS)». Outre ce renvoi, l'accord ne comporte – contrairement au précédent – plus ses propres dispositions en matière de protection des données. Pour cette raison, nous avions, dans notre prise de position sur le projet d'accord, retenu qu'il fallait une base légale pour la communication des données personnelles, à l'exemple de l'accord précédent. Celle-ci devrait également réglementer le traitement des données personnelles, y compris leur collecte, les accès, la conservation et la suppression des données personnelles, le droit d'accès, etc. La référence prévue à la SORN renvoie au droit américain (une «notice»), qui devrait alors également être applicable lorsque des données personnelles sont communiquées par la Suisse aux États-Unis. La SORN pourrait toutefois être modifiée unilatéralement

par les États-Unis, sans influence possible par la Suisse. La Suisse serait simplement informée d'éventuelles modifications. Pour cette raison, nous avons considéré que la SORN n'était pas une base légale suffisante au sens de la LPD. Le fait que les États-Unis assurent dans l'accord que les données personnelles bénéficient de la même protection des données que dans l'accord conclu en 2007 entre les États-Unis et l'UE sur la communication des données de passagers n'y change rien non plus. De plus, les garanties en matière de protection des données y ont été encore plus assouplies, comme l'observe le Groupe de travail «article 29» sur la protection des données de l'UE dans une prise de position. Il aurait été en outre été souhaitable que la Suisse ait pu conclure un accord semblable avec les États-Unis, sans référence unilatérale au droit américain.

1.1.6 Conclusion d'un accord établissant une sphère de sécurité entre la Suisse et les Etats-Unis («U.S-Swiss safe harbor framework»)

Les Etats-Unis ne disposent pas d'une protection des données d'un niveau adéquat, de sorte que le transfert de données personnelles vers une entreprise aux Etats-Unis nécessite que les deux parties conviennent de garanties spéciales. En collaboration avec le Secrétariat d'Etat à l'économie (SECO), nous avons élaboré avec les Etats-Unis un ensemble de règles garantissant un niveau suffisant de protection des données pour les entreprises enregistrées. Ainsi, le transfert de données entre les entreprises suisses et les entreprises américaines enregistrées est considérablement facilité.

La législation américaine n'offre pas une protection des données adéquate du point de vue de la législation suisse. Ceci implique que les entreprises établies en Suisse ne pouvaient jusqu'ici transmettre des données personnelles à leurs partenaires américains que sur la base d'accords mutuels. Ces accords devaient nous être soumis auparavant pour examen. Les données personnelles pouvaient ensuite être transmises vers l'entreprise aux Etats-Unis. Il existe déjà un accord dit de «sphère de sécurité» (ou «safe harbor») en matière de protection des données entre l'Union européenne et les Etats-Unis, que le PFPDT considère comme une simplification du processus. Pour cette raison, les Etats-Unis nous ont demandé si la Suisse désirait y adhérer. Désormais, avec ce nouvel accord conclu avec le Ministère du commerce américain, le PFPDT a mis sur pied en collaboration avec le SECO, dans le cadre du Forum de coopération sur le commerce et les investissements avec, un nouvel instrument qui simplifie le transfert de données entre la Suisse et les Etats-Unis pour les entreprises.

A l'avenir, en s'adressant au Département américain du commerce, les entreprises américaines pourront se faire enregistrer dans cet accord établissant une sphère de sécurité entre les Etats-Unis et la Suisse. Elles s'engagent ainsi à respecter les principes de protection des données qui y sont consignés. Pour les entreprises enregistrées, cet accord garantit un niveau de protection adéquat aux Etats-Unis. Il facilite la libre circulation des données entre les entreprises suisses et les entreprises américaines. La Communauté européenne dispose d'un régime similaire depuis 2000.

Ce régime permettra dorénavant aux entreprises suisses de ne devoir ni négocier un contrat avec un partenaire américain enregistré, ni en informer le PFPDT. Les droits des personnes concernées seront également renforcés, le «U.S.-Swiss Safe Harbor Framework» prévoyant des instances spéciales de règlement des différends en cas de violation des droits en matière de données personnelles. De plus, la Federal Trade Commission pourra intervenir aux Etats-Unis en cas de violations sérieuses et répétées et prendre des mesures contre les entreprises enregistrées. Le Département américain du commerce fournit une liste de ces entreprises sur son site web (www.export.gov/safeharbor).

Avec le «U.S.-Swiss Safe Harbor Framework», le SECO et le PFPDT ont mis au point avec les Etats-Unis une base qui facilite d'une part la transmission des données personnelles entre les deux pays et qui renforce d'autre part renforce les droits de protection des données des personnes concernées.

1.2 Protection des données – Questions d'ordre général

1.2.1 Vidéosurveillance respectueuse de la protection des données grâce au chiffrement

La vidéosurveillance est en constante évolution. Grâce aux diverses méthodes de cryptage des images et à la division des clés de chiffrement, il est possible de développer des technologies respectueuses de la protection des données et d'éviter d'éventuels abus. Les accords entre développeurs et producteurs permettent de mieux diffuser ces technologies.

Dans notre dernier rapport d'activités, nous avions présenté une technologie pour une vidéosurveillance respectueuse de la protection des données (cf. notre 15e rapport d'activités, ch. 1.2.3). Ces nouvelles technologies, qui utilisent la méthode du chiffrement (images cryptées) continuent à se développer.

A la méthode du chiffrement, les développeurs ont à présent ajouté la possibilité de diviser la clé de déchiffrement en deux parties physiquement séparées. Cette nouvelle caractéristique permet de garantir le principe des quatre yeux en transmettant les deux parties de la clé à deux personnes différentes, ce qui limite substantiellement les abus possibles. Cette propriété est très appréciée par les utilisateurs finaux. En outre, les développeurs ont conclu un accord avec une multinationale qui produit un logiciel de gestion des systèmes de vidéosurveillance (similaire au système de vidéosurveillance basé sur le réseau, cf. ch. 1.2.2). Il est ainsi désormais possible d'intégrer ce genre de caméras dans un produit de gestion standard. Grâce à ce genre d'accord, les développeurs ont la possibilité de mieux diffuser leurs caméras.

Nous encourageons le développement et la diffusion de technologies et de produits respectueux de la protection des données.

1.2.2 Système de vidéosurveillance basé sur le réseau

Grâce aux développements techniques de ces dernières années, les systèmes de vidéosurveillance ont beaucoup évolué, passant d'un modèle simple avec une caméra et un écran à des systèmes plus complexes comprenant plusieurs caméras, posées à divers endroits et surveillées par différents utilisateurs. Si l'évolution de la technique a conduit à une prolifération des systèmes de vidéosurveillance, de nouveaux produits permettant de garantir une meilleure protection des données sont aussi apparus sur le marché.

Il y a encore quelques années, les systèmes de vidéosurveillance se limitaient à de simples caméras et des opérateurs qui regardaient les images en temps réel. L'évolution de la technique intervenue ces dernières années, en particulier la diffusion d'Internet et des caméras numériques, permet désormais d'élaborer des systèmes plus complexes. Si d'un côté cette évolution a provoqué une prolifération des systèmes de vidéosurveillance, d'un autre côté des systèmes respectueux de la protection des données sont aujourd'hui disponibles.

Les systèmes modernes de vidéosurveillance peuvent ainsi compter plusieurs centaines de caméras distribuées dans le monde entier. Grâce à leur diffusion par Internet, les images parviennent à de nombreux utilisateurs dans plusieurs centrales de surveillance. Ces utilisateurs peuvent avoir des tâches, des responsabilités et des droits différents. Les systèmes de vidéosurveillance doivent permettre la gestion de toutes ces variables. Les images ne sont plus directement envoyées aux utilisateurs, mais réunies dans une base de données centrale à laquelle ces derniers peuvent accéder. La protection de cette base de données – ainsi que du serveur qui l'héberge – joue un rôle fondamental.

Dans le cadre de nos activités de surveillance, nous avons suivi le développement de la technique et examiné en particulier un système de vidéosurveillance basé sur le réseau, comportant les caractéristiques suivantes:

- Les communications des images entre les caméras et le serveur de même que entre le serveur et les utilisateurs sont chiffrées. Ceci empêche des accès non autorisés et permet d'utiliser Internet comme moyen de communication sans risque d'atteinte à la personnalité.
- Même si un chiffrement robuste serait l'idéal, un codage des images dans la base de données garantit un niveau minimal de sécurité, en particulier si l'accès physique et logique au serveur est aussi protégé.

- Pour des accès très sensibles, par exemple l'accès au serveur, il est possible de choisir une double clé (principe des quatre yeux).
- Il est possible de définir quelles caractéristiques de la caméra (par exemple le zoom, la rotation, l'activation du microphone, etc.) sont à disposition de quels utilisateurs. En outre il est possible de définir quels droits ont les différents utilisateurs (par exemple voir les images, les exporter, déclencher une alarme, etc.).
- Une journalisation des accès permet de savoir qui (quel utilisateur) a fait quoi (par exemple voir des images) et quand.
- La possibilité d'intégrer différents modèles de caméras permet une grande flexibilité et le changement des caméras en cas de nécessité.

Nous estimons qu'un tel produit permet de concilier les intérêts légitimes de la vidéosurveillance avec ceux de la protection des données, en particulier si les caméras choisies permettent un chiffrement à la base robuste (cf. ch. 1.2.1).

1.2.3 Guide relatif aux systèmes de reconnaissance biométrique

Nous avons élaboré un guide destiné aux développeurs et exploitants de systèmes de reconnaissance biométrique. Celui-ci est subdivisé en trois parties: La première apporte des précisions terminologiques, la seconde énumère les principes directeurs applicables à la conception et à l'utilisation de tels systèmes; la dernière partie comprend un guide comprenant une liste des questions à se poser dans le cadre de l'évaluation de tels systèmes et qui énumère les exigences du point de vue de la protection des données.

Suite à de nombreuses questions dans le domaine de la biométrie, et en particulier suite à notre recommandation de décentralisation des données biométriques au centre sportif KSS (cf. ch. 1.2.4), nous avons établi un document relatif aux systèmes de reconnaissance biométrique. Celui-ci est subdivisé en trois parties: la partie introductive est consacrée en particulier à la terminologie et aux définitions relatives à la biométrie et nécessaires à une bonne compréhension d'une matière aussi complexe; la deuxième partie énumère et explicite les principes directeurs applicables lors de la conception et de l'utilisation de systèmes de reconnaissance biométrique; la troisième et dernière partie consiste en un guide comprenant une liste des questions à se poser dans le cadre de l'évaluation de tels systèmes et qui énumère en conséquence les exigences que ceux-ci doivent remplir du point de vue de la protection des données.

S'agissant de la terminologie, il convient de distinguer les processus biométriques d'enrôlement (enregistrement d'une référence biométrique personnelle), et ceux de vérification (d'une identité) et d'identification (d'une personne). Sur la base de différentes caractéristiques biométriques (physiologiques ou comportementales) sont tirées des données biométriques brutes, d'où sont extraites des données dérivées ou gabarits biométriques. Ces derniers permettent de vérifier une identité ou d'identifier la personne concernée sur la base de la comparaison biométrique entre le gabarit de référence et le gabarit d'épreuve. Du fait de la nature probabiliste de toute comparaison biométrique, le seuil d'acceptation choisi conditionne le taux de fausses acceptations (lorsqu'une personne est identifiée comme une autre) et le taux de faux rejets (lorsque la personne enregistrée n'est pas reconnue), et donc la fiabilité du système.

Les principes directeurs mentionnés dans la deuxième partie du guide, à savoir la licéité, la proportionnalité, la finalité et la transparence des traitements biométriques, l'exactitude (ou la qualité) et la sécurité des données biométriques, ainsi que les droits des personnes concernées, trouvent leur fondement dans la LPD.

Concernant le guide d'évaluation, la première série de questions porte sur la finalité du système de reconnaissance, sur la nature du processus de reconnaissance (vérification ou identification) et sur les modalités de stockage des données biométriques. La deuxième série de questions concerne les moyens de reconnaissance biométrique, soit les modalités utilisées (biométriques et/ou traditionnelles), les traces, la nature (brute ou dérivée) et la sensibilité des caractéristiques biométriques choisies. La troisième série de questions aborde les aspects de sécurité des données et de fiabilité du système, en analysant l'architecture du système, les mesures de sécurité et le fonctionnement des processus d'enrôlement et de reconnaissance, y compris leur configuration et efficacité technique. Enfin, la quatrième et dernière série de questions résume les droits des personnes concernées et les conditions du devoir de déclaration du fichier biométrique constitué.

1.2.4 Suivi du contrôle au centre sportif KSS

Suite au refus du centre sportif KSS de suivre l'une de nos recommandations, nous avons porté le cas auprès du Tribunal administratif fédéral pour décision.

Suite à nos recommandations adressées au centre sportif KSS à Schaffhouse (cf. notre 15e rapport d'activités 2007/2008, ch. 1.2.5), ce dernier nous a indiqué qu'il refusait de mettre en œuvre notre recommandation relative au stockage décentralisé des données biométriques.

Lors du stockage de données personnelles dans une base de données centralisée, les personnes concernées ne sont plus en mesure de contrôler l'utilisation de leurs données. Or, le principe de proportionnalité prévoit que tout traitement de données personnelles doit être effectué à l'aide de moyens nécessaires, aptes à atteindre le but recherché, et non excessifs au regard des finalités. Dans le cas d'espèce, nous sommes d'avis que le stockage des données biométriques dans une base de données centralisée constitue une atteinte disproportionnée aux droits des personnes concernées au regard des finalités du traitement.

La décentralisation des données biométriques peut être réalisée à l'aide de différentes technologies. Il existe divers types de supports permettant aux personnes concernées de contrôler, en partie ou en totalité, l'usage qui est fait de leurs données personnelles. Dans le cas KSS, nous avons recommandé la mise en œuvre d'une solution intermédiaire (comparaison biométrique sur carte – «match on card») offrant un contrôle partiel. Ce type de support permet de stocker les données biométriques sur une carte personnelle et de réaliser le processus de comparaison sur cette dernière.

Vu le refus de KSS de mettre en œuvre notre recommandation, nous avons porté l'affaire devant le Tribunal administratif fédéral. Nous sommes actuellement dans l'attente de sa décision.

1.2.5 Traitement de données par des instituts de recherche de marché et sociales

Soucieuse de respecter les principes de la LPD et de se démarquer ainsi de certaines entreprises peu sérieuses actives dans le domaine du marketing direct, l'Association suisse des spécialistes en recherches de marché et sociales nous a contactés pour nous soumettre diverses questions de protection des données et pour s'assurer que ses méthodes ainsi que sa documentation sont bien conformes à la législation suisse. Nous avons répondu aux questions posées et proposé à la branche diverses améliorations. L'association a suivi nos remarques et adapté ses règlements et directives internes.

L'Association suisse des spécialistes en recherches de marché et sociales (ASMS) représente les intérêts de sa branche, au nom de ses membres individuels et collectifs, dont font partie en particulier les principaux instituts actifs dans le domaine de la recherche sociale et de marché. Y sont également représentés les chercheurs d'instituts spécialisés dans le domaine de la recherche de marché, de l'opinion publi-

que et sociale, les conseils indépendants en publicité ou chefs de marketing au sein d'entreprises ou d'organisations qui ont une activité liée à la recherche de marché, de même que les professeurs et les étudiants en sciences sociales.

Les recherches de marché et sociales permettent de collecter les informations les plus diverses sur la vie économique, culturelle et politique d'un pays ou d'une région. Dans le cadre d'une enquête de marché ou d'un sondage d'opinion, les personnes issues de la population sont sollicitées à donner leur avis tout personnel sur de nombreux sujets et elles participent à une telle enquête sur une base volontaire. L'évaluation de ces informations permet entre autres d'effectuer une photographie des opinions politiques dans une Suisse démocratique, de faire le point sur l'évolution sociale et culturelle, ou encore d'évaluer et d'optimiser des produits et services, en d'autres termes de mieux comprendre le fonctionnement d'une société donnée et de saisir comment pense et agit la population ou les différents groupes qui la composent. Les entreprises ont recours aux recherches de marché pour analyser les comportements de consommation et d'achat et pour ainsi mieux répondre aux besoins et aux souhaits des consommateurs. Pour prendre des décisions importantes, entreprises, organisations et autres associations mais aussi décideurs politiques, partis et administrations se réfèrent aux données obtenues dans le cadre de ces enquêtes.

Les instituts de recherche de marché et sociale se réclamant de la marque collective garantissent qu'aucune enquête n'est effectuée dans un but publicitaire, de vente ou de commande, clairement affiché ou caché. De même, les directives de l'ASMS garantissent que les données ne sont communiquées à leurs mandants ou à des tiers qu'après avoir été anonymisées, de sorte qu'une identification des personnes concernées ne peut être déduite de leurs réponses. Les personnes acceptant de participer à une enquête partent du principe que leurs données sont évaluées par l'institut de recherche et anonymisées au plus tard lors de la transmission des résultats de l'étude à des tiers.

Dans ce cadre, l'ASMS nous a soumis le problème auquel elle est actuellement confrontée: les mandants de l'ASMS souhaitent à présent, à des fins de contrôle qualité, écouter des interviews ou des discussions de groupe et recevoir des documents ou des informations qui permettraient d'identifier les personnes concernées. Or, il s'avère qu'une communication des données personnelles (non anonymisées) à des tiers dans un but de contrôle de qualité représente un changement de finalité et doit être clairement reconnaissable pour la personne concernée et être justifiée par un motif justificatif (en principe le consentement).

Nous avons recommandé à l'ASMS d'adapter ses réglementations internes et ses contrats en conformité avec la législation sur la protection des données. L'Association a suivi nos remarques et procédé aux modifications nécessaires.

1.2.6 Echange de données entre caisse de pension et administration fiscale

Nous avons effectué une expertise sur la question de savoir si une caisse de pension enfreint les dispositions légales de protection des données lorsque, chaque année, elle communique des attestations de rentes et de prestations à l'administration fiscale, conformément à une obligation légale de communication. Nous sommes parvenus à la conclusion qu'il y a une base légale pour une obligation de présenter une attestation tant en droit fiscal qu'en droit des assurances. Ni l'art. 86a al.1 let. e LPP ni l'art. 19 al. 4 LPD ne sont applicables en cas d'obligations légales de communiquer.

Se fondant sur l'art. 172 al. 1 let. b de la loi cantonale sur les impôts (LI), l'administration fiscale du canton de Berne a requis que lui soient fournies annuellement des attestations sur les rentes et les prestations versées. L'introduction du nouveau certificat de salaire est allée de pair avec celle d'un formulaire dénommé attestation de salaire et de rente. Sur la base de cette nouvelle réglementation, l'autorité cantonale de taxation demande désormais que ces attestations lui soient fournies annuellement.

La représentante légale de la caisse de pension a considéré qu'il y avait là un conflit entre l'art. 172 al. 1 let. b LI et l'art. 129 al. 1 let. b de la loi fédérale sur l'impôt fédéral direct (LIFD) d'une part et les art. 17 et 19 LPD et l'art. 86a al. 1 let. e de la loi fédérale sur la prévoyance professionnelle (LPP) d'autre part.

Nous avons établi une expertise afin de déterminer si, en communiquant annuellement ces attestations à l'autorité cantonale comme la loi le lui impose, la caisse de pension enfreignait des dispositions du droit de la protection des données.

Nous avons vérifié en premier lieu si, conformément à l'art. 17 al. 1 LPD, la collecte de données reposait sur une base légale permettant à l'autorité fiscale de demander des données sur les rentes. Nous avons constaté que pour la remise des attestations de rentes et de prestations il existait une base légale pour une obligation de communiquer tant à l'art. 172 al. 1 let. b LI qu'à l'art. 129 al. 1 let. b LIFD. Outre la législation sur les impôts, la législation sur la prévoyance professionnelle prévoit, à l'art. 81 al. 3 LPP et à l'art. 8 de l'ordonnance sur les déductions admises fiscalement pour les cotisations versées à des formes reconnues de prévoyance (OPP 3), une obligation légale d'attester à l'égard des autorités fiscales. Etant donné que l'obligation d'attester est expressément réglée dans les lois fiscales, la communication des données ne viole pas l'art. 19 al. 1 LPD.

Nous avons ensuite examiné la question de savoir si l'art. 19 al. 4 LPD permettait de restreindre la communication de données autorisée. La norme spéciale figurant dans la LPP ayant la primauté, il fallait déterminer si la caisse de pension serait autorisée à restreindre ou refuser la communication de données en se fondant sur la disposition de protection des données de l'art. 86a al.1 let. e LPP. Ainsi qu'il résulte de l'interprétation, l'art. 86a LPP a été créé à la suite de l'introduction de la législation sur la protection des données de la Confédération. A cette occasion, les dispositions de protection des données de la LPP ont été adaptées à la LPD. Jusqu'à la loi du 23 juin 2001 sur l'adaptation et l'harmonisation des bases légales pour le traitement de données personnelles dans les assurances sociales, la communication de données et les exceptions au devoir de discrétion étaient régies dans l'ordonnance du Conseil fédéral du 7 décembre 1987.

Pour des raisons de sécurité et d'uniformisation du droit, plusieurs modifications ont été introduites dans les lois sur les assurances sociales. Dans le domaine de la LPP, les adaptations ont été effectuées par le rajout de l'art. 86a. L'art. 86a al. 1 let. e LPP se réfère à la communication de données et correspond par analogie à l'art. 1 al. 1 de l'ordonnance sur les exceptions à l'obligation de garder le secret dans la prévoyance professionnelle et sur l'obligation de renseigner incombant aux organes de l'AVS/AI (OSRPP) alors en vigueur qui régissait l'obligation de renseigner. Cette disposition faisait la différence entre une communication de données dans les cas individuels faisant suite à une demande écrite et dûment motivée, cas dans lesquels les données sont communiquées sans problème sur demande, et les cas dans lesquels il n'est pas nécessaire de disposer d'un consentement pour communiquer les données. Si la caisse de pension pouvait restreindre ou refuser sa communication de données en se fondant sur l'art. 86a al. 1 let. e LPP, on pourrait invoquer le motif justificatif de l'intérêt privé prépondérant. Selon la jurisprudence du Tribunal fédéral, ces intérêts privés prépondérants doivent toutefois toucher la personne de l'assuré lui-même, l'employeur ou d'autres personnes impliquées. Il s'agit en premier lieu de données relatives à la santé, à la situation professionnelle ou aux secrets d'affaires. Pour cette raison, selon notre conclusion, l'art. 86a al. 1 let. e LPP n'est applicable que si une autorité transmet une demande de renseignement à une fondation de prévoyance en faveur du personnel, dans le cadre de l'entraide administrative. L'autorité de taxation ne doit pas émettre de demande de renseignement dans le cadre d'attestations de rentes qu'il faut fournir en vertu d'une obligation de communiquer établie par la loi. La caisse de pension n'a pas d'obligation de renseigner, mais est soumise à une obligation spéciale d'attester selon laquelle elle doit envoyer les attestations à l'autorité de taxation sans y être invitée.

Au vu de ce qui précède, nous estimons que l'autorité de taxation n'enfreint ni l'art. 17, ni l'art. 19 LPD car, en vertu des art. 172 al. 1 let. b LI, de l'art. 129 al. 1 LIFD ainsi que de l'art. 81 al. 3 LPP et de l'art. 8 OPP 3, elle entreprend la collecte des données fiscales de manière licite.

De même, conformément aux art. 172 al. 1 let. b LI et 129 al. 1 let. b LIFD, la caisse de pension n'est pas soumise à une obligation de renseigner, mais à une obligation de communiquer, raison pour laquelle dans ce contexte, ni l'art. 86a al. 1 let. e LPP, ni l'art. 19 al. 4 LPD ne sont applicables. La caisse de pension n'enfreint donc pas le devoir de discrétion en transmettant les attestations de rente.

1.2.7 Transmission de données personnelles à des tiers par les autorités fédérales

Une autorité fédérale peut communiquer des données personnelles sur demande à des tiers à condition que cette communication repose sur une base légale. Sans base légale, l'autorité peut également communiquer le nom, le prénom et la date de naissance d'une personne mais doit ce faisant tenir compte d'éventuels besoins de protection selon le contexte ou la personne.

Les autorités fédérales nous ont demandé si elles pouvaient également transmettre à des tiers des données personnelles sans l'autorisation des personnes concernées.

Selon l'art. 19 al. 1 LPD, les organes fédéraux ne sont en droit de communiquer des données personnelles que s'il existe une base légale au sens de l'art. 17 LPD ou – notamment – que la personne concernée y a, en l'espèce, consenti; ou que si le destinataire rend vraisemblable que la personne concernée ne refuse son accord ou ne s'oppose à la communication que dans le but de l'empêcher de se prévaloir de prétentions juridiques ou de faire valoir d'autres intérêts légitimes (par exemple pour se soustraire au paiement de dettes); dans la mesure du possible, la personne concernée doit être auparavant invitée à se prononcer.

Nous avons souligné que la prescription légale mentionnée est une disposition potestative, ce qui signifie que l'organe de la Confédération n'est pas obligé de communiquer les données.

Par ailleurs, un organe fédéral peut en vertu de l'art. 19 al. 2 LPD communiquer le nom, l'adresse et la date de naissance d'une personne même si les conditions de l'art. 19 al. 1 LPD ne sont pas remplies. En conséquence, ces données peuvent être communiquées sans consentement et sans consultation. Cette disposition est aussi une disposition potestative qui ne peut obliger l'organe fédéral à renseigner.

Mais selon le contexte ou la personne, la communication d'un nom, d'une adresse ou d'une date de naissance peut se traduire par une atteinte aux droits de la personnalité ou aux droits fondamentaux. Pour cette raison, les organes de la Confédération doivent tenir compte des éventuels besoins de protection lors de la communication de données selon l'art. 19 al. 2 LPD.

1.2.8 Publication d'avis de recherche et de disparition sur des sites web privés

La publication d'avis de recherche policiers sur Internet se justifie par l'intérêt public d'appréhender rapidement la personne et d'empêcher des délits. Cette justification disparaît toutefois après un certain temps, au plus tard après l'arrestation ou la découverte de la personne recherchée, et les données personnelles correspondantes doivent être retirées du réseau.

Notre attention a été attirée par des tiers sur un site web qui publie notamment des avis de recherche policiers, des rapports sur des délits et des avis de disparition. Les données personnelles de suspects, d'auteurs et aussi de victimes y sont rendues publiques. Les textes datent en partie d'il y a plusieurs années.

La publication de données personnelles sur Internet représente un traitement de données au sens de la loi fédérale sur la protection des données et nécessite un motif justificatif. Ce dernier peut être le consentement de la personne concernée, un intérêt privé ou public prépondérant, ou une base légale.

La publication d'un avis de recherche policier sur Internet se justifie par un intérêt public prépondérant (appréhension de la personne, empêchement d'autres délits, etc.). Il existe en outre des bases légales au niveau cantonal qui légitiment en principe une telle publication. Ces publications relèvent en effet de la compétence des autorités cantonales de protection des données.

L'intérêt public pour de telles publications disparaît toutefois au plus tard lorsque la personne recherchée a été trouvée. Ainsi, il n'existait plus aucun motif justificatif pour la plupart des documents publiés sur le site web en question, sauf si les personnes concernées avaient donné leur consentement, ce que rien ne permet cependant de supposer.

Les personnes concernées par la publication peuvent exiger de l'exploitant du site web que leurs données soient bloquées. Cette exigence peut également être imposée par une procédure de droit civil. Les personnes concernées peuvent en outre demander des dommages-intérêts pour atteinte à la personnalité.

Nous avons prié l'exploitant du site web de rendre inaccessible, sans délai, les données personnelles pour lesquels il n'existe pas (plus) de motif justificatif.

1.2.9 Transmission de listes de signatures par l'autorité indépendante d'examen des plaintes en matière de radio-télévision

A l'occasion d'une plainte populaire, l'autorité indépendante d'examen des plaintes en matière de radio-télévision a transmis la liste des signatures aux responsables de l'émission incriminée sans y avoir été invitée. Bien que nous ayons établi que dans le cas concret, la LPD n'était pas applicable, les questions de protection des données ne sont pas sans importance. Nous avons informé l'autorité indépendante que l'action de transmettre la liste des signatures sans y avoir été invitée ne reposait sur aucune base légale. En outre, nous avons souligné qu'il serait du devoir du législateur par exemple d'adapter la loi fédérale sur la radio et la télévision dans le cadre d'une éventuelle révision.

Une personne a déposé une plainte dite populaire auprès de l'autorité indépendante d'examen des plaintes en matière de radiotélévision (AEIP). Pour ce genre de plaintes, il faut notamment déposer, avec la plainte, une liste comportant les signatures de vingt personnes. L'AEIP a transmis la plainte et la liste aux responsables de l'émission en question.

Il s'agissait d'examiner ici si la transmission de la liste de signatures constitue une violation des principes de la loi sur la protection des données. Nous avons prié l'AEIP, qui avait déjà demandé auparavant à l'Office fédéral de la justice (OFJ) une brève analyse sur ce point, de prendre position. L'OFJ a nié l'application de la loi sur la protection des données dans le cas d'espèce, d'une part parce qu'il s'agissait d'une procédure en cours et d'autre part parce qu'il ne s'agissait pas d'une procédure de première instance. Nous partageons cet avis. Ceci ne signifie pas pour autant que les questions de protection des données ne jouent ici aucun rôle.

Nos recherches ont révélé que dans la pratique, l'AEIP transmet la liste de signatures avec la copie de la plainte aux responsables de l'émission en question. Ce faisant, elle communique des données personnelles. En qualité d'organe de la Confédération,

l'AEIP ne doit communiquer des données personnelles que si cette communication repose sur une base légale, à moins que des dispositions dérogatoires ne soient prévues dans d'autres lois. La loi fédérale sur la radio et la télévision (LRTV) ne contient aucune base légale permettant la communication de la liste de signatures. Nous avons informé l'AEIP que sa pratique actuelle, consistant à transmettre sans y avoir été invitée la liste de signatures, n'était pas conforme à la loi sur la protection des données. Il serait du devoir du législateur d'adapter la LRTV sur ce point, par exemple dans le cadre d'une éventuelle révision.

A titre complémentaire, nous avons précisé qu'à notre avis, il existe une base légale pour une communication des données personnelles dans le cadre du droit de consulter les dossiers. Avant de trancher si le droit de consulter les dossiers selon l'art. 27 al. 1, let. b, de la loi fédérale sur la procédure administrative (PA) doit être refusée ou non, il faudrait dans le cas d'espèce procéder à une pesée des intérêts en jeu avant la communication. Toutefois, l'examen de la question de savoir si et dans quelles circonstances le droit de consultation des données doit être refusé ou non relève des tribunaux.

1.2.10 Règlement de traitement: procédures de contrôle

Les règlements de traitement doivent être établis et tenus à jour conformément aux directives. Ils doivent, entre autres, mentionner les procédures de contrôle. La plupart des règlements ne comportent toutefois aucune indication à ce sujet. Des audits devraient cependant régulièrement être menés, en particulier sur les systèmes sensibles.

Nous devons malheureusement encore une fois constater que souvent les règlements de traitement ne sont pas tenus de manière conforme aux directives. Dans certains cas, nous avons trouvé que les règlements étaient plutôt bons au début, mais n'avaient plus été mis à jour par la suite. Souvent, nous avons pu constater sur la base des règlements de traitement qu'aucun contrôle interne ou externe n'avait été effectué, notamment pendant l'exploitation des fichiers. Ceci est regrettable, car c'est justement en phase d'exploitation que d'importantes conclusions peuvent être tirées pour optimiser le système, entre autres aussi dans le domaine de la protection des données. Des contrôles ou audits réguliers sont donc très importants, puisqu'ils fournissent au maître de fichier de nouveaux enseignements d'importance, qui lui permettront de prendre les décisions adéquates. Le règlement de traitement doit assurer la transparence. Ce n'est que sur la base d'informations transparentes qu'il est possible de contrôler les systèmes de manière appropriée.

Les éléments devant figurer dans un règlement de traitement se trouvent dans le document intitulé «Que doit donc contenir un règlement de traitement?» sur notre site web www.leprepose.ch, sous la rubrique Documentation – protection des données – brochures – mesures techniques et organisationnelles.

1.3 Internet et télécommunication

1.3.1 Bourses d'échange sur Internet: Action auprès du Tribunal administratif fédéral

La recommandation adressée à une entreprise active dans le domaine de la lutte contre les violations du droit d'auteur sur les bourses d'échange (réseaux pair à pair) a été soumise au Tribunal administratif fédéral (TAF) pour décision (cf. notre 15e rapport d'activités 2007/2008, ch. 1.3.1). Après deux échanges d'écriture, on attend la décision du TAF.

1.3.2 Protection des jeunes sur Internet

Les mineurs ne peuvent remettre de déclaration de protection des données sans l'accord de leur représentant légal. Ce fait peut poser des problèmes aux exploitants de sites Internet, notamment lorsque les jeunes s'enregistrent sur leur site (par ex. pour un jeu de loterie). Supposer le consentement implicite des parents dans le cadre de l'utilisation d'Internet peut être problématique. Nous conseillons donc aux exploitants de requérir le consentement des représentants légaux.

Il est pratiquement impossible pour les exploitants de sites Internet de contrôler l'identité de leurs visiteurs dans le monde virtuel. Cet état de fait peut être une source de problèmes considérables, surtout dans le domaine de la protection de la jeunesse. En effet la question se pose de savoir comment obtenir l'accord des représentants légaux, en particulier pour les exploitants de sites Internet destinés aux enfants et jeunes et prévoyant un enregistrement. Nous avons reçu une demande de conseil et avons cherché à savoir comment obtenir un consentement juridiquement valable en vue du traitement de données de personnes mineures âgées de 12 à 16 ans.

Conformément à la loi fédérale sur la protection des données, les personnes concernées doivent donner leur consentement au traitement de leurs données personnelles lorsque ce traitement le requiert. Un exploitant de sites Internet peut prévoir l'enregistrement de ses visiteurs pour que ceux-ci puissent par exemple adhérer à un service de réseautage social ou participer à un jeu-concours. Néanmoins, pour traiter les données personnelles, il a besoin d'un consentement (sauf s'il peut se fonder sur une base légale ou sur un intérêt prépondérant privé ou public). En général, cela ne pose aucun problème puisque les personnes s'enregistrent en leur nom propre et

que l'on peut ainsi supposer qu'il y a au moins consentement implicite (pour autant que l'information préalable soit suffisante). Mais lorsque le site web s'adresse à des personnes mineures, la question se pose de savoir si et dans quelle mesure celles-ci peuvent remettre une déclaration de consentement juridiquement valable.

Il ne peut en principe y avoir consentement que si la personne concernée a l'exercice de ses droits civils, c'est-à-dire qu'elle a atteint l'âge de la majorité et qu'elle est capable de discernement. Conformément au code civil suisse, c'est le cas des personnes physiques uniquement lorsqu'elles ont atteint l'âge de 18 ans révolus. Auparavant, pour les actes générateurs d'obligations (donc tous les actes juridiques faisant naître une charge ou un renoncement à des droits), elles ont besoin du consentement de leur représentant légal. Le souci de protection de la personne mineure joue ici un rôle déterminant. Le représentant légal peut accorder un consentement général pour toute une série d'actes générateurs d'obligations à condition que l'on puisse garder sur ces actes une bonne vue d'ensemble et que l'on puisse estimer leurs répercussions potentielles. Il ne doit donc pas donner son consentement pour chacun des actes juridiques que la personne mineure conclut.

Reste à savoir si l'autorisation accordée par les représentants légaux pour l'utilisation d'Internet peut permettre de supposer qu'il y a implicitement un consentement juridiquement valable pour le traitement des données personnelles que les mineurs divulguent volontairement sur Internet. Pour ce qui est des jeunes âgés de douze à seize ans, à notre avis, la réponse est non. Du fait que la protection des données a pour objectif le respect des droits de la personnalité, de l'avis du PFPDT, on ne peut se baser ici sur les capacités des mineurs capables de discernement dans leurs rapports avec les biens dont ils disposent librement (argent de poche). Lorsque des mineurs s'enregistrent sur un site web et remettent une déclaration de protection des données, nous estimons que les représentants légaux doivent donner leur consentement.

Or, des parents qui reçoivent, de façon inopinée, de l'exploitant d'un forum Internet un courrier par lequel on leur demande de donner leur consentement à l'utilisation du forum peuvent se trouver irrités par cette démarche. Nous conseillons donc d'agir comme suit.

Dans un premier temps, après information préalable, l'exploitant d'un forum Internet ne devrait demander que l'adresse du mineur, à la suite de quoi il peut écrire aux parents. En parallèle, le mineur devrait confirmer qu'il a demandé le consentement à ses parents. De son côté, l'exploitant devrait attirer l'attention du mineur sur le fait que les parents auront à confirmer ce consentement dans les jours qui suivent, par poste et par écrit. Cela a pour but d'inciter le mineur à demander le consentement

de ses parents avant ou pendant son inscription. Ainsi, ces derniers seront informés et ne seront pas surpris par un courrier inattendu. Si les parents donnent leur accord, l'utilisation peut être validée. S'ils ne donnent pas leur consentement dans un certain délai, toutes les données introduites devront être effacées.

1.3.3 Evaluation en ligne de praticiens de la santé

Suite à de nombreuses plaintes relatives au site d'évaluation en ligne de praticiens de la santé www.okdoc.ch, nous avons procédé à un établissement des faits et précisé les exigences en matière de protection des données dans le cadre de l'évaluation en ligne anonyme de praticiens de la santé.

La mise en ligne en mai 2008 d'un site d'évaluation des praticiens de la santé www.okdoc.ch a suscité de nombreuses plaintes de la part de praticiens de la santé.

Suite à ces plaintes, nous avons procédé à un établissement des faits conformément à l'art. 29 LPD auprès de la société gérant le site d'évaluation, Bonus SA, et lui avons émis des recommandations en juin 2008. Ces dernières portaient en particulier sur la nécessité du consentement des praticiens concernés et sur la possibilité pour ces derniers de s'opposer non seulement aux évaluations mais également à la mention des données de fait (nom, spécialisation et adresse).

Après avoir émis nos recommandations et organisé une séance avec le responsable de Bonus.ch, ladite société a procédé à une réorientation de son site, à savoir la transformation du site d'évaluation en un site de recommandation.

Lors du suivi de l'implémentation de nos recommandations, nous avons précisé les conditions que doit remplir le nouveau site de recommandation afin d'être conforme avec la législation sur la protection des données:

- Les évaluations et les commentaires positifs peuvent être conservés dans la mesure où ils concernent des praticiens qui ne se sont pas opposés au traitement de données en question après avoir reçu un courrier d'information (consentement tacite).
- La réactivation des modalités de recommandation pour les praticiens qui se sont opposés à être évalués n'est possible que si, suite à la réception d'un courrier d'information, ils consentent expressément à ce que l'évaluation paraisse sur le nouveau site.

- De même, les données de fait doivent en principe être retirées du site dans la mesure où les praticiens concernés l'ont demandé. Elles ne pourront être réintroduites au cas par cas que si, suite à l'envoi de la lettre d'information, un médecin qui avait préalablement requis le retrait des données de fait le concernant demande expressément que celles-ci soient réintroduites.

Bonus.ch a introduit ces points dans la section intitulée «Consentement tacite et droit d'opposition» du courrier d'information adressé aux praticiens de la santé. L'envoi par Bonus.ch d'un courrier d'information à tous les praticiens de la santé s'inscrit dans le cadre du suivi de la mise en œuvre de nos recommandations.

1.3.4 Protection de la personnalité dans les comptes-rendus sur Internet

Pour déterminer si une information rapportée sur Internet contrevient aux droits de la personnalité des personnes concernées, il convient, selon le principe de la proportionnalité, de peser les intérêts en présence, à savoir l'intérêt public attaché à l'événement d'un côté et de l'autre l'intérêt à la sphère privée des personnes concernées. Devrait être mis en avant dans le compte-rendu l'événement lui-même et non une personne en particulier assistant à l'événement et à laquelle aucun intérêt public n'est rattaché. La mise à l'index d'une personne dans un compte-rendu est en général considérée comme une atteinte illicite à la personnalité. Au cours de l'année écoulée, nous avons eu à juger plusieurs cas de la sorte. Ceux-ci nous ont incités à élaborer des directives dans le but de faciliter la pesée des intérêts à lumière du principe de la proportionnalité.

De plus en plus de comptes-rendus de manifestations, accompagnés de photos des personnes présentes sont publiés sur des sites web. Cela va de la relation d'événements de moindre importance dans le cadre d'une association aux informations concernant de très grandes manifestations rapportées dans les médias imprimés et numériques. A cet égard, la question se pose souvent de savoir s'il est licite de représenter des personnes de façon à ce qu'on puisse les reconnaître et à partir de quel moment cette représentation porte atteinte aux droits de la personnalité. Pour y répondre, il faut procéder à une pesée entre l'intérêt public au rapport de l'information et l'intérêt à protéger la sphère privée des personnes concernées, à la lumière du principe de la proportionnalité. Au cours de l'année écoulée, nous avons élaboré des directives dont le but est de faciliter une telle pesée des intérêts.

D'une manière générale, les visiteurs et les participants des manifestations publiques doivent s'attendre à figurer d'une manière ou d'une autre dans un compte-rendu, qu'il s'agisse d'une mention ou d'une photographie. En effet, ce genre de manifestations relève de l'intérêt public. Cela dit, toutes les formes de compte-rendu ne sont pas licites. Ainsi, les textes et les images doivent se limiter pour l'essentiel aux aspects qui relèvent de l'intérêt public (la manifestation elle-même, les incidents particuliers, etc.) et qui préservent au mieux la personnalité des personnes présentes. Il faut y veiller lors de la rédaction des textes et du choix des photographies. Les comptes-rendus portant sur des personnes publiques ainsi que ceux qui présentent le caractère de la manifestation dans ses traits essentiels ne posent en général pas de problèmes. Par contre, il n'est généralement pas admis que les informations soient concentrées sur des personnes qui ne sont pas particulièrement au cœur de la manifestation et qui n'ont pas donné leur consentement à ce genre de compte-rendu. Si en outre certaines personnes ou groupes de personnes (peut-être même avec mention des noms) sont mis à l'index, il y a alors dans la plupart des cas une atteinte illicite à la personnalité.

De nombreux organisateurs informent sur leurs sites web les participants à leur manifestation de la possibilité de ce genre de comptes-rendus et de la communication de données personnelles à des tiers. Nous avons constaté que certains organisateurs parviennent à obtenir des participants d'importants droits d'utilisation des données personnelles. Ils utilisent des clauses de consentement très générales et en font une condition obligatoire d'inscription. Nous estimons cependant ce procédé illicite; en effet la portée du traitement des données n'est pas transparente pour le participant et celui-ci n'est ainsi pas informé de manière adéquate. De plus, on ne peut pas dans tous le cas exiger l'acceptation de telles clauses de consentement, notamment dans le cadre du marketing (cf. ch. 1.8.5).

Dans beaucoup de cas cependant, des particuliers assistant à une manifestation sont photographiés (souvent à leur insu) et leurs données personnelles sont ainsi publiées sur Internet. S'il n'existe aucun intérêt public majeur à la représentation de la personne, il y a atteinte illicite à la personnalité car les personnes concernées ne doivent pas s'attendre à ce genre de compte-rendu. Pour elles, le traitement de données n'est pas manifeste et l'on ne peut soutenir qu'elle y ont implicitement consenti. Ainsi, à l'occasion d'un compte-rendu anonyme de la Fête de Sempach, certains participants supposés appartenir à l'extrême droite ont vu paraître leurs portraits sur le site www.indymedia.ch et ont été de ce fait mis à l'index.

Dans certains cas, un compte-rendu anonyme permet qu'une opinion soit exprimée librement. Il constitue de ce fait une composante importante de la liberté de la presse et doit à notre avis demeurer fondamentalement possible. Les journalistes et les reporters devraient toutefois veiller à éviter les atteintes à la personnalité.

Un autre problème se pose avec l'hébergement des pages Internet à l'étranger (hors de l'Europe) car les personnes concernées ne disposent pas dans ce cas de voie de droit effective. Nous attirons une fois de plus l'attention sur les difficultés qu'il y a à appliquer une protection des données efficace face à un média de portée mondiale tel l'Internet. Pour cette raison, nous demandons que des règles générales soient mises en place à l'échelle internationale afin d'améliorer la protection des données.

1.3.5 Outils d'évaluation pour les sites web

Sur mandat de l'administration fédérale et suite à diverses demandes émanant de particuliers, nous avons analysé les outils d'évaluation de sites web sous l'angle de la protection des données. A notre avis, différentes conditions doivent être remplies lorsque des outils d'évaluation sont utilisés pour établir des statistiques d'accès à des sites web. En particulier, il faut signaler à l'utilisateur, dans une déclaration de protection des données, que des données le concernant sont collectées et lui indiquer à qui elles sont transmises (y compris l'indication du pays). Si les données sont acheminées vers un pays dont le niveau en matière de protection des données n'est pas adéquat, il faut convenir, avec le prestataire de l'outil d'évaluation, des garanties qui assurent un niveau de protection suffisant.

Un nombre toujours croissant d'exploitants de sites web décident de ne plus établir leurs statistiques eux-mêmes sur la base de programmes installés sur leurs serveurs. Ils font désormais compter les visites sur leurs sites par des outils en ligne (par ex. Google Analytics). Les adresses IP devant être considérées comme des données personnelles, la loi fédérale sur la protection des données (LPD) est applicable. Donc, pour utiliser ces outils d'évaluation en conformité avec le droit de la protection des données, les exploitants de sites web doivent veiller à respecter en particulier les points décrits ci-après.

L'outil d'évaluation en ligne est intégré au site web de l'exploitant à l'aide d'un élément d'image spécial ainsi que d'un script du prestataire. Ainsi, le prestataire de l'outil d'évaluation saisit les accès sur le site, car l'adresse IP de l'utilisateur est enregistrée par son serveur lors de l'appel de l'élément d'image. Les données accessoires de l'utilisateur Internet qui apparaissent lors de la visite du site sont transmises au prestataire de l'outil d'évaluation. Sous l'angle de la protection des données, ce processus doit être considéré comme un traitement de données par des tiers. Conformément à l'art. 10a LPD, le traitement de données par un tiers est possible si une convention le

prévoit et que le prestataire traite les données comme l'exploitant du site lui-même serait autorisé à le faire et qu'aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

Pour cette raison, l'exploitant d'un site doit obliger par contrat le prestataire de l'outil d'évaluation à utiliser les données livrées exclusivement dans le but d'évaluation qui est celui de l'exploitant (et non pas à d'autres finalités propres au prestataire) et à assurer la sécurité des données. En outre, l'exploitant du site web doit, sur la base du principe de reconnaissabilité, attirer l'attention des utilisateurs, dans la déclaration de protection des données, sur l'outil d'évaluation ainsi que sur le genre et le volume des données traitées.

Si les serveurs du prestataire de l'outil d'évaluation se trouvent à l'étranger, il convient en outre de respecter les règles légales auxquelles est soumis le transfert des données au-delà des frontières. En effet, les données personnelles ne doivent pas être communiquées à l'étranger si la personnalité des personnes concernées s'en trouve gravement menacée, notamment s'il n'y existe pas de législation garantissant une protection adéquate (une liste des pays et de leur niveau en matière de protection des données peut être consultée sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – transmission à l'étranger). Dans ce cas, l'outil d'évaluation ne peut être utilisé que si le prestataire assure un niveau adéquat de protection en donnant des garanties suffisantes (art. 6 al. 2 let. a LPD). Dans la pratique, ces garanties sont en général données par une confirmation écrite du prestataire. Depuis janvier 2009, le «U.S.-Swiss Safe Harbor Framework» constitue un instrument visant à garantir un niveau de protection suffisant pour les données transférées vers les Etats-Unis (pour plus d'informations, cf. ch. 1.1.6).

Tant que l'exploitant d'un site web observe ces points, rien – du point de vue de la protection des données – ne s'oppose à l'utilisation d'un outil d'évaluation. Néanmoins, les exploitants de sites web devraient en principe évaluer dans quelle mesure il est pour eux souhaitable de transmettre à l'étranger les données personnelles des visiteurs de leur site. Les autorités étrangères pourraient en effet, sur la base de leurs législations nationales, accéder aux données se trouvant dans leur pays.

1.3.6 Observations concernant les sites de réseautage social

Les sites de réseautage social (SRS) sont aujourd'hui très à la mode et leurs utilisateurs augmentent de jour en jour. Depuis longtemps déjà, ces personnes échangent sur ces sites toutes sortes d'informations personnelles et il n'est pas rare qu'ils établissent d'eux-mêmes des profils de la personnalité qu'ils mettent à la disposition d'autres utilisateurs. Ce faisant, ils négligent souvent les risques que comportent ces SRS. Nous avons donc décidé d'examiner ces risques de plus près afin de donner quelques conseils aux utilisateurs de ces sites. Nos «observations concernant les sites de réseautage social» figurent en annexe (ch. 4.1.1) ou peuvent être consultés sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – internet.

1.3.7 Observations concernant les sites d'évaluation sur Internet

Les évaluations sur Internet de groupes professionnels divers (médecins, professeurs, enseignants, etc.) sont devenus de plus en plus populaires. Une évaluation en ligne pouvant porter atteinte à la personnalité de l'individu évalué, nous avons décidé d'analyser plusieurs sites d'évaluation. Au terme de nos analyses, nous avons mis au point des principes portant sur la structure et l'utilisation des sites d'évaluation dans le but de fournir des conseils utiles aux utilisateurs, aux administrateurs de ces sites et aux personnes concernées. Ce rapport peut être consulté en annexe (ch. 4.1.2) ou sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – internet.

1.3.8 Explications concernant la télévision numérique

L'offre de films numériques ne cesse d'augmenter, que ce soit sur Internet ou par les liaisons à large bande. Alors qu'avec la diffusion terrestre traditionnelle des programmes, il était possible de demeurer un consommateur anonyme d'émissions de télévision et de films, un canal ascendant à haut débit est disponible pour la télévision numérique et la télévision par Internet, grâce auquel il est théoriquement possible de déterminer les habitudes de consommation des téléspectateurs. Ces nouvelles technologies sont très intéressantes, en particulier pour la publicité qu'il est ainsi possible de personnaliser. Dans nos explications consacrées à la télévision numérique, nous en avons analysé les risques et les dangers et donné des conseils aux consommateurs et aux fournisseurs de services numériques sur la manière d'utiliser au mieux ce média. Le rapport complet peut être consulté en annexe (ch. 4.1.3) ou sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – autres thèmes.

1.3.9 Explications concernant les systèmes «Pay as you drive»

La minimisation et la prévention des risques figurent parmi les préoccupations essentielles des assurances automobiles. Depuis l'année dernière, une compagnie suisse d'assurances propose un contrat spécialement pour les jeunes conducteurs. Grâce à une boîte noire qui enregistre les mouvements du véhicule juste avant et après un accident, ils obtiennent un rabais de prime considérable, pouvant aller jusqu'à 30%. Il est, grâce aux technologies aujourd'hui disponibles, théoriquement pensable d'enregistrer et donc de surveiller le comportement de conduite des automobilistes. Nous avons examiné la problématique des systèmes dits «Pay as you drive» sous l'angle de la protection des données. Le rapport détaillé peut être consulté en annexe (ch. 4.1.4) ou sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – assurances.

1.4 Justice/Police/Sécurité

1.4.1 Schengen

Les rapports concernant la mise en oeuvre de Schengen ainsi que nos activités dans ce domaine se trouvent sous le chiffre 1.9.

1.4.2 Entrée en vigueur de la loi fédérale sur les systèmes d'information de police de la Confédération

La loi fédérale sur les systèmes d'information de police de la Confédération met sous un même toit les bases légales régissant une grande partie des fichiers de police exploités au niveau fédéral. Dans le domaine du droit d'accès, toutes les demandes de renseignements concernant ces fichiers doivent être adressées directement à l'Office fédéral de la police.

La loi fédérale sur les systèmes d'information de police de la Confédération (LSIP) est entrée en vigueur le 5 décembre 2008. Cette loi s'applique aux fichiers de police exploités par la Confédération à l'exception du fichier GEWA du Bureau de communication en matière de blanchiment d'argent, du fichier ISIS du Service d'analyse et de prévention (rattaché depuis le 1er janvier 2009 au Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports, DDPS), du fichier fondé sur les profils d'ADN, du fichier AFIS contenant les images des empreintes digitales et du fichier ISA relatif aux documents d'identité. En ce qui concerne le fichier GEWA, la loi sur le blanchiment d'argent (LBA) dispose que le droit des particuliers d'obtenir des renseignements est régi par l'article 8 de la LSIP.

Cette nouvelle législation prévoit que les demandes d'accès au fichier JANUS, qui regroupe des données relatives au crime organisé ou au trafic des stupéfiants et à la traite des êtres humains, ainsi qu'au fichier GEWA, qui porte sur la lutte contre le blanchiment d'argent, doivent être adressées directement à l'Office fédéral de la police (fedpol) et non plus à notre secrétariat. Nous demeurons cependant encore très actifs dans ce domaine, notamment dans le traitement des demandes de vérification concernant les deux fichiers susmentionnés et dans le traitement des demandes de levée du report de la réponse lorsque celui-ci pourrait léser gravement et de manière irréparable la personne concernée. Pour plus de détails concernant les modalités d'accès aux fichiers JANUS et GEWA nous renvoyons à notre 15e rapport d'activités 2007/2008, ch. 1.4.4.

1.4.3 Visions locales relatives à l'exploitation pilote de l'index national de police

Les visions locales que nous avons effectuées et la documentation que nous a fourni l'Office fédéral de la police nous ont permis de constater que l'exploitation pilote de l'index national de police respectait les exigences de la loi fédérale sur la protection des données et celles de l'ordonnance sur l'exploitation pilote de l'index national de police.

En collaboration avec l'Office fédéral de la police (fedpol), nous avons effectué en février 2008 des visions locales auprès de le section de fedpol responsable de l'exploitation pilote de l'index national de police, de la centrale d'engagement de fedpol, de la centrale de renseignements à Berne du Corps des gardes-frontière et du commandement de la police cantonale bernoise. Cette dernière vision locale a été effectuée avec la collaboration du délégué à la protection des données du canton de Berne. Les visions locales avaient principalement pour but de vérifier que les exigences de la loi fédérale sur la protection des données et celles fixées dans l'ordonnance sur l'exploitation pilote de l'index national de police étaient bien respectées. Dans le cadre de ces visions locales, nous avons analysé notamment les données traitées, les accès à l'index et la sécurité des données.

En ce qui concerne les traitements des données personnelles, fedpol nous a confirmé que les catégories «AFIS ADN» et «INTERPOL» du système informatisé de gestion et d'indexation de dossiers et de personnes de l'Office fédéral de la police (fichier IPAS) et le système informatisé de la Police judiciaire fédérale (fichier JANUS) étaient raccordés à l'index dans le cadre de l'exploitation pilote. Les visions locales ont démontré que les utilisateurs avaient accès aux données prévues par l'ordonnance sur l'exploitation pilote de l'index national de police, à savoir: les données d'identification, la date de l'inscription, le motif de l'inscription lorsqu'une personne a fait l'objet d'un relevé signalétique, l'indication de l'autorité auprès de laquelle des informations supplémentaires peuvent être demandées et l'indication du système dont les informations sont issues.

Dans le cadre de l'exploitation pilote de l'index national de police, environ 500 autorisations d'accès individuelles ont été octroyées à des utilisateurs de la Confédération (environ 300 accès) et des cantons (environ 200 accès). Vu le nombre final d'utilisateurs de l'index national de police (environ 5'000 pour l'administration fédérale, les cantons et les communes), l'octroi de 500 autorisations d'accès individuelles lors de l'exploitation pilote paraît raisonnable.

Sur le plan de la sécurité des données, l'accès à l'index bénéficie de différentes mesures de sécurité. Toutes les transmissions de données sont chiffrées et toutes les activités sont journalisées.

En conclusion, nous avons, sur la base des visions locales effectuées et de la documentation fournie, constaté que l'exploitation pilote de l'index national de police respectait les exigences de la loi fédérale sur la protection des données et celles de l'ordonnance sur l'exploitation pilote de l'index national de police.

1.4.4 Demandes d'accès concernant le système d'information ISIS

Le nombre des demandes d'accès concernant le système d'information ISIS a connu une augmentation fulgurante en 2008. C'est d'ailleurs la première fois que nous avons pu à informer de manière appropriée quelques-uns des requérants sur l'existence d'enregistrements. Il serait souhaitable qu'un droit d'accès direct soit introduit pour ISIS, tel que cela vient d'être fait pour JANUS et GEWA.

Le nombre des demandes d'accès appelées indirectes concernant la base de données ISIS (sûreté intérieure) a énormément augmenté en 2008. Ainsi, nous avons reçu 148 demandes d'accès en 2008, comparé à 19 l'année précédente. Cette hausse vertigineuse a deux raisons principales.

Nous avons pour la première fois pu appliquer la règle d'exception prévue par la loi, qui nous permet d'informer de manière appropriée les personnes fichées dans ISIS sur les données qui les concernent. En effet, la loi correspondante prévoit que nous nous limitions à donner en principe une réponse standard, au libellé toujours identique. Cette réponse ne permet pas à la personne concernée de savoir si des informations la concernant ont été enregistrées dans ISIS. Celle-ci sait uniquement que le PFPDT a examiné sa demande et qu'il a émis une recommandation de rectification à l'intention de l'office au cas où des irrégularités auraient été décelées. La clause d'exception prévue par la loi qui permet de fournir plus d'informations doit cependant être interprétée de manière très stricte et doit être vérifiée séparément pour chaque cas. Dans les cas précités, il s'agissait entre autres de plusieurs requérants qui avaient fait valoir en même temps leur droit d'accès au système ISIS. Tous ces requérants se doutaient, suite à certains événements, qu'ils avaient été fichés dans la base de données. Notre enquête a révélé que les faits mentionnés par les requérants n'avaient pas mené à des enregistrements dans ISIS. Pourtant, quelques-uns d'entre eux étaient fichés pour d'autres raisons. Après avoir examiné chaque demande, nous avons conclu que les conditions d'application de la règle d'exception de la LMSI (lésion grave et irréparable et absence de menace pour la sûreté intérieure ou extérieure) étaient remplies dans

chacun de ces cas. Nous avons donc informé les requérants de manière adéquate. Ces personnes ont partiellement rendu ces informations publiques et incité d'autres personnes à faire valoir également leur droit d'accès au fichier ISIS. Il convient à cet égard de relever que nous sommes bien sûr tenus d'examiner de cas en cas si les conditions permettant de ne pas devoir donner une réponse standard sont réunies.

Une autre fait qui a déclenché une vague de demandes d'accès à ISIS fut la publication par les médias de cas concernant certains membres du Grand Conseil du canton de Bâle-Ville. Comme cela a été communiqué dans la presse, la Commission de gestion de Bâle-Ville avait, semble-t-il, constaté que des données concernant quelques membres du Grand-Conseil d'origine kurde avaient été communiquées au Service d'analyse et de prévention (SAP) de l'Office fédéral de la police.

Plusieurs litiges en rapport avec le système d'information ISIS sont actuellement pendants auprès du Tribunal administratif fédéral. Nous sommes bien sûr intéressés de voir comment le tribunal va trancher.

Depuis le 1er janvier 2009, le service SAP, responsable du système ISIS, ne fait plus partie de l'Office fédéral de la police, mais du Département de la défense, de la protection, de la population et des sports (DDPS). Nous présumons que ceci n'entravera pas la bonne collaboration que nous avons entretenue jusqu'ici.

Comme nous l'avons mentionné au ch. 1.4.2 du présent rapport d'activités, les bases de données JANUS et GEWA sont dorénavant assujetties au droit d'accès direct. Il serait souhaitable qu'un régime similaire soit mis en place aussi rapidement que possible pour ISIS. Nous nous sommes toujours prononcés contre le droit d'accès «indirect» et sommes d'avis qu'un droit d'accès direct est bien plus opportun.

1.4.5 Introduction de données biométriques dans les documents d'identité

Plusieurs demandes nous ont été adressées en rapport avec le référendum contre l'arrêté fédéral du 13 juin 2008 portant approbation et mise en oeuvre de l'échange de notes entre la Suisse et la Communauté européenne concernant la reprise du Règlement (CE) 2252/2004 relatif aux passeports biométriques et aux documents de voyage (Développement de l'Acquis de Schengen). Nous avons renvoyé à notre position (cf. 15e rapport d'activités 2007/2008, ch. 1.1.3) en rappelant d'une part que le règlement susmentionné ne prévoit pas la conservation des données biométriques au-delà du temps nécessaire à l'établissement des documents et d'autre part que nous ne soutenons pas la conservation centralisée des données biométriques dans les fichiers relatifs aux documents d'identité.

1.4.6 L'utilisation de profils d'ADN dans les procédures pénales et à des fins d'identification de personnes inconnues ou disparues

Dans le cadre de notre fonction d'autorité de surveillance en matière de protection des données, nous avons procédé à un examen des faits auprès de l'Office fédéral de la police (fedpol). Il en ressort que la protection des données a été intégralement respectée lors des traitements qui ont fait l'objet de l'examen.

Dans le cadre de l'examen des faits, nous avons contrôlé le service de coordination ADN (qui exploite la banque de données CODIS), la division «Services AFIS ADN» (qui exploite la banque de données IPAS) ainsi que la plateforme de communication «Message Handler». Nous avons demandé qu'on nous remette surtout des documents relatifs au traitement des données, aux différents processus et aux flux de données que nous avons ensuite analysés.

Lors d'une visite auprès du service de coordination ADN à l'Institut de médecine légale de l'Université de Zurich-Irchel et de la division «Services AFIS ADN» dans les locaux de l'Office fédéral de la police, nous avons eu l'occasion de voir comment les données sont traitées.

L'examen des faits a mis en évidence les points suivants:

Les autorités de poursuite judiciaire à tous les échelons se voient confrontées à des formes modernes de criminalité, caractérisées par une mobilité élevée, une spécialisation accrue, un travail d'équipe et l'engagement de moyens techniques. Dans le cadre de la lutte contre ces nouvelles formes de criminalité, il est très important entre autres d'identifier rapidement et avec certitude les criminels ou les bandes criminelles, et de déceler les activités criminelles et les éléments communs à diverses infractions au-delà des frontières cantonales et nationales. Ceci inclut une évaluation systématique de toutes les traces, y compris des traces biologiques, par exemple une identification au moyen de profils d'ADN.

Le 1er janvier 2005, la loi fédérale sur l'utilisation de profils d'ADN dans les procédures pénales et sur l'identification de personnes inconnues ou disparues (loi sur les profils d'ADN) est entrée en vigueur. Cette loi fixe les conditions auxquelles les profils d'ADN peuvent être utilisés dans des procédures pénales et traités dans un système d'information fédéral. La loi règle en outre l'identification par la comparaison de profils d'ADN de personnes inconnues, disparues ou décédées, en dehors d'une procédure pénale.

Le profil d'ADN est un code alphanumérique propre à chaque individu qui est établi, à l'aide de techniques de biologie moléculaire, à partir des séquences non codantes du matériel génétique ADN, et qui permet d'identifier avec certitude une personne.

C'est l'autorité de poursuite (police cantonale) ou l'autorité chargée de l'enquête pénale qui lance la procédure d'identification au moyen d'un profil d'ADN. C'est également elle qui procède aux examens préliminaires sur la base des empreintes digitales, qui prélève les frottis de muqueuse jugale, sauvegarde les traces relevées sur le lieu de l'infraction et mandate l'analyse du profil.

Au début du processus de traitement, la police attribue un numéro de contrôle de processus au matériel biologique. Ce numéro unique, attribué une seule fois à chaque frottis de muqueuse jugale ainsi qu'à chaque trace relevée sur le lieu de l'infraction, permet la pseudonymisation et le suivi sans équivoque de la procédure, depuis le prélèvement du matériel jusqu'à l'effacement des données, respectivement la destruction du matériel.

Le matériel biologique est remis au laboratoire d'analyse forensique par la poste, par coursier ou directement par la police. Le laboratoire contrôle et confirme la réception de chaque trace et de chaque frottis de muqueuse jugale. La police met à disposition du laboratoire les informations relatives au cas dont il a besoin pour l'examen des traces.

Le laboratoire crée les profils d'ADN des frottis de muqueuse jugale et des traces relevées sur le lieu de l'infraction et les transmet au service de coordination ADN. L'échantillon biologique est détruit au plus tard après 3 mois.

Le service de coordination ADN, sis dans les locaux de l'Institut de médecine légale de Zurich, exploite la banque de données de profils d'ADN CODIS (Combined DNA Index System) pour le compte de la Confédération. Il réceptionne les profils d'ADN établis par le laboratoire ou remis par la Police judiciaire fédérale (demandes émanant d'Interpol), les enregistre dans CODIS, procède à une comparaison automatisée avec les profils qui y figurent déjà et évalue les résultats.

Il y a concordance lorsque le profil d'une personne et une trace relevée sur le lieu où a été commis une infraction se recoupent. Les concordances contribuent à l'élucidation d'un ou de plusieurs cas, à la charge ou à la décharge des personnes concernées. Le service de coordination ADN remet le résultat définitif de la recherche sous forme du numéro de contrôle de processus (de la recherche et de la concordance) à la division «Services AFIS ADN» de fedpol.

A la fin de l'année 2007, la banque de données CODIS contenait 92'912 profils de personnes et 17'346 traces relevées sur des lieux où ont été commises des infractions. Les concordances suivantes ont été obtenues:

personne-trace: 3'210 concordances

personne-personne (jumeaux monozygotes): 17 concordances

trace-trace: 4'809 concordances (ces concordances fournissent des informations précieuses sur les éléments communs à diverses infractions)

La division «Services AFIS ADN» reçoit les résultats de la recherche sous forme de numéro de contrôle de processus. Les résultats sont automatiquement reliés avec les données relatives aux personnes ou au cas qui s'y réfèrent dans IPAS. Le rapport complet ainsi que sa liste de distribution sont contrôlés, corrigés et si nécessaire complétés par la division «Services AFIS ADN». Le rapport est ensuite mis en circulation conformément à la liste de distribution.

A la fin du processus d'examen, la police peut consulter ce rapport, l'imprimer ou l'intégrer directement dans ses propres constats de police. Si nécessaire, elle transmet ces informations aux autorités judiciaires compétentes. La demande de radiation est faite par la police, soit de sa propre initiative, soit sur mandat des autorités judiciaires compétentes. Le service de coordination ADN effectue ensuite les radiations demandées dans CODIS. La sécurité du transfert des données est garantie par une plateforme de communication spécialement créée à cet effet.

Les banques de données CODIS (profils d'ADN) et IPAS (données relatives aux cas et aux personnes) sont séparées aussi bien sur le plan physique qu'organisationnel, et ne peuvent – en cas de concordance – être reliées l'une à l'autre qu'au moyen du numéro de contrôle de processus. Le service de coordination ADN et la division «Services AFIS ADN» procèdent régulièrement à des comparaisons des données contenues dans les banques de données CODIS et IPAS.

Dans le cadre de notre examen des faits, nous avons constaté que les exigences de la protection des données ont été intégralement respectées lors des traitements qui ont fait l'objet de l'examen.

1.4.7 Systèmes de reconnaissance faciale dans les stades de sport

Nous avons été invités à prendre position sur deux des aspects du projet «Sécurité dans le sport». Il s'agissait avant tout des sujets «Recours à la biométrie ou à des dispositifs de reconnaissance faciale aux entrées d'un stade» et «Mise en relation des enregistrements vidéo dans les stades avec la biométrie ou la reconnaissance faciale». Le recours à des systèmes de reconnaissance faciale dans les stades est autorisé selon la loi sur la protection des données lorsque certaines conditions sont respectées.

Des représentants de la Confédération, de cantons et de fédérations sportives se sont réunis autour d'une «Table ronde pour lutter contre la violence dans le sport». Dans ce contexte, l'un des groupes de travail de la table ronde nous a demandé de prendre position sur deux des aspects du projet «Sécurité dans le sport». Il s'agissait avant tout des sujets «Recours à la biométrie ou à des dispositifs de reconnaissance faciale aux entrées d'un stade» et «Mise en relation des enregistrements vidéo dans les stades avec la biométrie ou la reconnaissance faciale». Nous avons indiqué que la loi fédérale sur la protection des données est applicable lorsque des données personnelles sont traitées par des personnes privées (exploitants de stades privés) ou des organes fédéraux (Office fédéral de la police). Par contre, les lois cantonales sur la protection des données s'appliquent au traitement des données par des organes cantonaux (p. ex. police cantonale, police municipale). Dans de tels cas, l'appréciation des aspects liés à la protection des données est de la compétence du délégué cantonal (ou municipal) à la protection des données. Notre prise de position (ci-après) se rapporte donc uniquement au traitement des données par des personnes privées et des organes fédéraux. En règle générale, il s'agit d'observer les principes généraux de la protection des données (licéité, proportionnalité, finalité, etc.). Les personnes privées doivent donc présenter un motif justificatif pour le traitement de données personnelles, à savoir le consentement de la personne concernée, un intérêt prépondérant public ou privé, ou une loi. Pour leur part, les organes fédéraux sont autorisés à traiter des données personnelles lorsqu'une base légale existe.

Pour le recours à la biométrie ou à des dispositifs de reconnaissance faciale aux entrées d'un stade, le groupe de travail pour le projet pilote nous a fait part de certaines contraintes. Le but du projet est d'éviter la violence en reconnaissant les personnes sous le coup d'une interdiction de stade ou d'une autre mesure au sens de l'art. 24a ss de la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI; interdiction de périmètre, interdiction de se rendre dans un pays donné, obligation de se présenter à la police, garde à vue), et en les empêchant de pénétrer dans le stade.

Les installations de reconnaissances faciales mises en œuvre sont des appareils semi-mobiles, installés dans différentes entrées du stade, ces emplacements n'étant pas connus à l'avance par les spectateurs. Le contrôle facial s'effectue alors plus au moins en même temps que le contrôle des personnes, et de manière reconnaissable pour les personnes concernées. Un spécialiste est toujours présent lors de la reconnaissance faciale.

Les photos introduites dans les installations de reconnaissance faciale proviennent d'une part de la base de données HOOGAN de l'Office fédéral de la police, d'autre part des listes d'interdictions de stade des clubs de sport ou fédérations sportives. Les données sont toujours séparées selon leur provenance. En particulier, aucune donnée HOOGAN n'est copiée dans les listes d'interdictions de stade.

Les données HOOGAN et les listes d'interdictions de stade sont remises sur des clés USB chiffrées séparées et enregistrées dans deux galeries séparées.

Les données HOOGAN présélectionnées par l'Office fédéral de la police ne sont enregistrées que juste avant la manifestation sportive, puis détruites immédiatement après sous le contrôle d'un représentant autorisé de la police. Les conditions applicables sont donc identiques à celles qui existent déjà aujourd'hui, à la différence près que les données ne sont pas fournies sur papier, mais sur une clé USB chiffrée. L'Office fédéral de la police adaptera en conséquence le règlement de traitement HOOGAN, ainsi que la directive HOOGAN.

Les photos enregistrées sont comparées avec les visiteurs pénétrant dans le stade (facetracking). S'il n'y a pas de concordance, les images des personnes entrantes ne sont pas enregistrées. En cas de concordance, ce qui se passe peut encore être configuré; une sortie imprimée devrait alors être faite dans tous les cas afin de disposer d'une preuve. Dans le projet pilote, il n'y aura pas non plus de «base de données biométriques».

Dans ce contexte, nous avons donné l'appréciation suivante des aspects liés à la protection des données:

Pour la transmission des données HOOGAN aux organisateurs et responsables de la sécurité, des bases légales (LMSI et ordonnance correspondante) existent. De plus, conformément aux bases légales, les données peuvent être traitées dans des systèmes électroniques de reconnaissance de personnes. Toutefois, le règlement de traitement et la directive HOOGAN devraient encore être adaptés, puisqu'ils prévoient une transmission sur papier et non sous forme électronique. Dans ce cadre, il importe en outre d'assurer premièrement que les données transmises soient consignées et deuxièmement que les données soient supprimées en toute sécurité au terme de la

manifestation sportive et qu'elles ne puissent pas être réutilisées. Nous constatons que la transmission de données sur une clé USB chiffrée doit, du point de vue de la protection des données, être considérée comme étant au moins équivalente à une transmission de données sur papier.

Pour la transmission de données provenant des listes d'interdictions de stade des clubs de sport et/ou des fédérations sportives à des organisateurs et responsables de la sécurité, l'existence d'un motif justificatif (intérêt prépondérant privé ou public) peut être affirmée. Toutefois, les principes généraux de la protection des données doivent là aussi être respectés. En particulier, les données personnelles ne peuvent être traitées que si elles ont été saisies de manière licite. A titre d'exemple, les photos de personnes sous le coup d'une interdiction de stade ne peuvent être traitées que si elles ont été prises de manière licite. C'est le cas lorsque les images ont été produites dans le cadre d'une surveillance vidéo à des fins de sécurité dans le stade et que les images enregistrées sont pertinentes en termes de sécurité (p. ex. violences).

De même, il existe en principe un motif justificatif (intérêt prépondérant privé ou public) pour la reconnaissance faciale lors d'un contrôle de personnes par des exploitants de stade ou leurs responsables de la sécurité. Les principes généraux de la protection des données sont là aussi applicables. Ainsi, selon le principe de proportionnalité, seules les données qui sont effectivement appropriées et nécessaires au but poursuivi peuvent être traitées. Par ailleurs, la sécurité des données doit être assurée au sens de la LPD. Selon la LMSI, il faut s'assurer en outre que les données HOOGAN ne sont pas mélangées à d'autres données et qu'elles sont effectivement supprimées après la manifestation. De plus, les spectateurs devraient être informés de la reconnaissance faciale par des panneaux indicateurs et éventuellement par une communication sur le billet d'entrée. L'impression d'une concordance à des fins de preuve est certainement admissible. Si le cas est transmis à la police cantonale, le traitement des données est, comme déjà mentionné, régi par le droit cantonal.

Nous avons attiré l'attention du groupe de travail sur le fait que ce n'est pas le PFPDT, mais les différentes personnes chargées du traitement des données (Office fédéral de la police, organisateurs selon la LMSI, etc.) qui restent responsables du respect de la législation en matière de protection des données. Finalement, nous nous sommes permis d'observer que nous doutions de l'efficience de l'installation; à notre avis la question de savoir si, étant donné les traitements de données prévus, le taux effectif de concordance de l'installation de reconnaissance faciale est suffisamment important pour justifier l'utilité de la mesure est contestable.

Enfin, nous avons attiré l'attention sur le fait que la reconnaissance faciale ne peut constituer un apport utile que si elle est combinée avec d'autres mesures (encadrement des supporters, recours à la police, etc.).

Quant à la mise en relation d'enregistrements vidéo dans le stade avec la biométrie ou la reconnaissance faciale, nous avons émis l'appréciation suivante:

Selon les indications du groupe de travail, il était également prévu de poursuivre la reconnaissance faciale pendant le jeu (après le contrôle d'entrée). Les dispositifs de reconnaissance faciale seraient alors connectés aux installations vidéo existantes dans les stades. Là aussi, les «non-concordances» ne seraient pas enregistrées. Le but serait d'annoncer d'éventuelles concordances à la police cantonale, qui rendrait ensuite visite à ces personnes.

Une telle pratique soulève la question de la proportionnalité. En tous les cas, les conditions mentionnées plus haut s'appliquent ici également. Le PFPDT n'est par ailleurs pas compétents pour apprécier les traitements de données effectués par la police cantonale.

Nous avons là aussi demandé au groupe de travail de s'assurer que, dans le cadre de son projet, les conditions de protection des données précitées soient respectées. Comme déjà mentionné, ce sont les différentes personnes chargées du traitement des données (Office fédéral de la police, organisateurs selon la LMSI, etc.) qui sont responsables du respect de la législation en matière de protection des données. Toutefois, la reconnaissance faciale devra être réévaluée après une certaine période par les organisateurs ou les responsables de la sécurité et la situation en matière de protection des données devra être vérifiée à nouveau sous l'aspect de la finalité et de la proportionnalité de la mesure.

Pour tous les autres points du projet pilote, par exemple sur la question de la reconnaissance faciale dans les lieux publics, nous n'avons pas pris position du fait que le groupe de travail ne les mentionnait qu'à titre accessoire et que le projet était encore insuffisamment concrétisé à nos yeux. D'autres problèmes en matière de protection des données, bien plus épineux, se posent et doivent encore être tirés au clair.

1.5 Santé

1.5.1 Transmission d'expertises médicales

La transmission d'une expertise médicale est une procédure délicate car elle consiste à transmettre des données personnelles particulièrement sensibles à un tiers. C'est pourquoi des bases légales spéciales claires existent dans certains cas pour la transmission intégrale d'expertises médicales sans le consentement explicite de la personne concernée. En l'absence de telles bases, les dispositions générales sur la protection des données doivent être respectées. Il y a lieu en particulier d'observer le principe de la proportionnalité.

Selon le principe de la proportionnalité, des données personnelles ne peuvent être traitées que dans la mesure où celles-ci sont objectivement appropriées et effectivement nécessaires pour atteindre un but déterminé. Même si elle est en principe autorisée à communiquer des informations, la personne transmettant une expertise médicale doit donc vérifier quelles indications elle peut remettre au destinataire concret. Si une expertise médicale contient des informations qui ne sont pas appropriées ni nécessaires pour atteindre le but concret du destinataire, la personne transmettant l'expertise doit supprimer ces informations ou les rendre méconnaissables. A défaut, il y a violation du principe de la proportionnalité. Ainsi, le «case manager» d'une assurance-accidents est en principe autorisé à transmettre des informations provenant d'une expertise à un assureur RC impliqué. Il doit cependant rendre dans le cas concret les indications non pertinentes pour l'assureur méconnaissables ou purement et simplement les supprimer. Il se peut ainsi par exemple que l'expertise établie par l'assurance-accidents contienne des indications sur les activités récréatives d'une personne ayant subi un dommage. Ces informations ne peuvent être transmises à l'assureur RC que si elles revêtent réellement une importance pour l'évaluation d'un recours. Cela est notamment le cas lorsqu'une personne ayant subi un dommage lors d'un accident de circulation pratique un loisir qui impliquerait des risques physiques particuliers et qui pourrait avoir influencé dans une large mesure le dommage physique subi lors de l'accident en question.

1.5.2 Base de données de patients en ligne

L'exploitation d'un fichier qui documente des évolutions de maladie de patients nécessite la mise en place de mesures de protection des données spécifiques. Ceci est particulièrement nécessaire dans les cas où le traitement est effectué en ligne. Les fonctions du traitement des données doivent être décrites et les personnes impliquées doivent être informées sur la procédure. L'objectif est de garantir par des mesures appropriées que les droits de la personnalité des patients sont protégés.

Les traitements de patients souffrant de maladies de longue durée engendrent des volumes de données considérables. Une des possibilités de traiter ces données consiste à les transférer dans un fichier par l'intermédiaire de formulaires papier. Une autre possibilité, que nous abordons ici, consiste à accéder aux données à travers un réseau public. Afin de pouvoir traiter les données, l'accès au fichier est accordé aussi bien aux médecins traitants qu'aux patients concernés. Les données traitées sont incontestablement des données sensibles. Cela signifie que leur traitement nécessite la mise en place de mesures particulières. Celles-ci peuvent être subdivisées en trois catégories: l'identification des acteurs, l'étendue de l'accès aux données et l'octroi des droits d'accès.

Un des systèmes qui nous a été présenté est un registre «à long terme» dans le domaine des maladies rhumatismales. Les mesures exigées et prises par l'exploitant doivent être considérées comme représentant le minimum requis pour une base de données de patients accessible en ligne.

- Identification du médecin ou du patient: suite à une demande d'accès faite par écrit, on vérifie les données du demandeur et on lui envoie ensuite par courriel un lien crypté qui lui permet d'activer son compte utilisateur.
- Étendue de l'accès aux données: une information à l'intention des patients décrit de manière précise quel médecin peut accéder aux données du patient. Un médecin peut accéder uniquement aux données de ses patients, un patient uniquement à ses propres données. Aussi bien le stockage que le transport des données est crypté.
- Octroi des droits d'accès: il n'a lieu qu'avec le consentement du patient. En cas de changement de médecin traitant, le patient peut décider si le médecin qui l'a traité jusqu'ici peut continuer à avoir accès à ses données. Si un patient quitte le système, toutes les données le concernant doivent à sa demande être supprimées.

Le processus présenté comporte deux éléments centraux: l'information du patient et la déclaration de consentement. Le patient est d'abord informé des buts du traitement et de la manière dont les données sont collectées et analysées, de même que de ce qui se passe en cas de changement de médecin traitant et des possibilités qu'a le patient de mettre fin au traitement des données. Le traitement des données ne pourra débuter qu'après avoir obtenu l'accord écrit du patient. Ce dernier peut d'ailleurs en tout temps révoquer son consentement sans encourir de préjudice.

1.5.3 Normes et architecture de la stratégie suisse en matière de cybersanté «eHealth»

Le 27 juin 2007, le Conseil fédéral a adopté la stratégie suisse en matière de cybersanté «eHealth». Celle-ci désigne entre autres deux objectifs: définir les standards nécessaires à la mise en œuvre de la stratégie ainsi qu'une architecture appropriée pour la cybersanté. Le mandat qui en résulte a été attribué au projet partiel «Normes et architecture». Les résultats de ce travail serviront de base aux autres projets partiels. C'est la raison pour laquelle nous avons décidé de collaborer activement à ce projet.

Certains événements dans le domaine de la santé en Suisse représentent un immense défi pour la protection des données. La mise en œuvre de la stratégie nationale en matière de cybersanté «eHealth», adoptée le 27 juin 2007 par le Conseil fédéral, fait sans aucun doute partie de ces défis.

Une protection des données efficace et effective repose sur la constatation qu'il faut lui accorder une importance qui soit en rapport avec la sensibilité des données personnelles traitées. Dans son papier stratégique, le Conseil fédéral accorde la plus haute priorité à la sécurité et à la protection des données. Pour lui, «le traitement de données médicales implique une intervention dans les droits fondamentaux et les droits de la personnalité des personnes concernées (p. ex. les patients). Pour que l'intervention soit légitime, des mesures légales, organisationnelles et techniques doivent être prises. La qualité de ces mesures a une forte influence sur la confiance que l'on accorde aux services électroniques de santé.»

Au vu de ces conditions préalables positives, nous avons décidé de collaborer activement aussi bien au projet partiel «Normes et architecture» qu'au projet partiel «Bases légales».

Le projet partiel «Normes et architecture» a pour but d'atteindre deux objectifs fixés par la stratégie:

- «D'ici à fin 2008, les normes d'un extrait électronique du dossier médical personnel, contenant les informations nécessaires au traitement, sont définies. Les conditions pour l'introduction sont décrites.»
- «D'ici à fin 2012, l'échange par voie électronique de données médicales entre les partenaires du système de santé est structuré et n'entraîne plus ni rupture de médias, ni pertes. Tous les hôpitaux de soins somatiques aigus, tous les réseaux de soins intégrés et au moins 50% des médecins libéraux ont adopté l'extrait électronique du dossier médical personnel qui comporte les informations importantes pour le traitement.»

Une des premières tâches a consisté à soumettre pour consultation aux cercles intéressés des propositions de mise en œuvre de la stratégie. Celles-ci incluent entre autres l'application des principes fondamentaux de la protection des données (pour de plus amples informations, voir www.ehealth.admin.ch). Il convient cependant de relever que les exigences de la protection des données ont déjà été intégrées dans les divers processus. En tant que principes et directives, elles représentent pour tous les acteurs une obligation non seulement sur le plan légal, mais également sur le plan organisationnel et technique. En bref, cela signifie que les processus de protection des données seront intégrés dans l'architecture «eHealth» sous forme «câblée».

Cela sera d'ailleurs bien nécessaire car il existe un intérêt vif pour les données de santé gérées de manière électronique, aussi de la part d'organisations qui ne peuvent pas faire valoir de droit légal à accéder à ces données. Le risque existe donc que l'exigence élevée du Conseil fédéral en matière de protection des données soit compromise. Ce risque doit être combattu non seulement en élaborant des normes utiles et une architecture adéquate, mais aussi en créant les conditions de base correspondantes aux niveaux politique et légal. C'est pourquoi la collaboration du PFPDT dans le projet partiel «Bases légales» est sans doute nécessaire. Nous continuerons à l'avenir à accorder une grande importance à la mise en œuvre de la stratégie du Conseil fédéral. Il est important, dans l'intérêt des patients, que nous saisissions avec eHealth l'opportunité de supprimer quelques-uns des chantiers existants dans le domaine de la santé publique plutôt que d'ouvrir de nouvelles fouilles.

1.5.4 Le consentement des personnes concernées lors de projets de recherche médicale

Les données pour la recherche doivent en principe être mises à disposition des chercheurs de manière anonyme. Dans la mesure où cela n'est pas possible, les personnes concernées doivent donner leur consentement. Si l'obtention du consentement n'est pas envisageable, il existe la possibilité d'effectuer les projets de recherche avec une autorisation de la Commission d'experts pour le secret professionnel dans la recherche médicale. Il existe aujourd'hui des systèmes qui prennent en compte différentes procédures permettant de mettre les données à disposition des chercheurs sous forme anonymisée.

La recherche avec des données personnelles médicales implique en principe toujours que l'on soit en possession du consentement du patient concerné, sauf si les données peuvent être mises à disposition des chercheurs sous forme anonymisée. Les données personnelles sont considérées comme anonymisées lorsqu'elles ne peuvent plus être attribuées à une personne identifiée ou identifiable. Sous cette forme, elles ne sont plus non plus soumises à la loi sur la protection des données. Dans la mesure où il n'est possible ni d'obtenir un consentement (par exemple parce que la personne concernée est décédée), ni d'effectuer la recherche avec des données anonymisées, il existe encore la possibilité de faire de la recherche à l'aide d'une autorisation générale ou d'une autorisation spéciale qui peut être délivrée par la Commission d'experts pour le secret professionnel dans la recherche médicale (Commission d'experts), avec les charges appropriées. Des contrôles de notre part, ainsi que des demandes de citoyens, ont toutefois mis en évidence que ces charges sont diversement interprétées. Certains présument qu'une autorisation de la Commission d'experts suffit notamment pour ne plus avoir à obtenir le consentement des personnes concernées. Une telle démarche est cependant illicite.

Le chercheur ne doit même pas entrer en contact avec des données personnelles, car celles-ci ne sont pas nécessaires aux projets de recherche. Il s'agit par conséquent de créer des systèmes appropriés qui permettent aux chercheurs de travailler avec des données anonymisées. L'anonymisation des données personnelles doit ou peut s'effectuer différemment selon la situation. Pour les données personnelles disponibles sur papier, il serait idéal de mettre à disposition du chercheur uniquement les données anonymisées par exemple par un collaborateur des archives. Ces documents pourraient aussi, selon les besoins, être complétés par un pseudonyme, de façon à ce que des résultats importants pour le patient puissent lui être communiqués.

La collecte de données de recherche à partir de base de données «électroniques» peut en principe s'effectuer sous forme anonyme, en prélevant les données du fichier de sorte qu'aucun élément identifiant ne soit repris dans l'ensemble des données de recherche. S'il s'avérait par la suite nécessaire d'accéder une nouvelle fois aux données d'origine, il serait là aussi possible de travailler avec des pseudonymes qui permettraient une réattribution des données d'origine.

Des solutions conformes à la protection des données existent aujourd'hui également pour les registres, tel que le registre du cancer. Des informations importantes sur l'anonymisation et la pseudonymisation dans le domaine médical se trouvent dans la série de publications de la «Telematikplattform für Medizinische Forschungsnetze» sous la référence «Generische Lösungen zum Datenschutz für die Forschungsnetze in der Medizin» (cf. www.tmf-net.de/Produkte/Uebersicht.aspx).

1.5.5 Collecte de données personnelles provenant des fichiers électroniques d'un hôpital à des fins de recherche

L'article qui suit présente une solution possible pour la collecte de données provenant de divers fichiers électroniques d'un hôpital et leur mise à disposition à des chercheurs, en conformité avec les exigences de la protection des données. En raison de la centralisation, une telle solution favorise aussi la transparence dans l'environnement de la recherche médicale de l'hôpital concerné.

Certains hôpitaux ont plusieurs fichiers électroniques dont les données permettent d'effectuer des projets de recherche. En toute logique, le chercheur s'adresse au maître de fichier pour qu'ils puissent collecter ensemble les données pertinentes. Ils doivent cependant veiller à ne collecter aucune donnée (directement) identifiante, telle que nom, prénom ou adresse. Le numéro qui identifie de manière biunivoque le patient à l'hôpital peut être collecté, mais ne doit pas être accessible au chercheur. Les données se trouvent alors sur un ordinateur portable et peuvent être transmises vers un ordinateur central du service de recherche. Celui-ci vérifie que les données (directement) identifiantes ont bien été éliminées. Si ce n'est pas le cas, le fait est consigné, puis communiqué au maître de fichier et au chef du projet de recherche. Par ailleurs, une autre séquence de caractères non interprétable (pseudonyme) est attribuée au numéro d'hôpital, de manière à permettre une éventuelle réidentification du patient au cas où celui-ci doit être informé en raison des résultats de la recherche. L'ordinateur du service de recherche possède également des enregistrements des personnes concernées qui ne souhaitent pas mettre leurs données personnelles à disposition.

Le système vérifie l'existence de données transmises à l'ordinateur relatives à des patients ayant bloqué leurs données pour les projets de recherche. Si de telles données existent, elles sont supprimées du système. Ce n'est qu'au terme de ces processus que les données sont mises à disposition des chercheurs. Ceux-ci ont alors un accès en ligne au système et peuvent effectuer leurs recherches. Il va de soi que les zones sensibles d'un tel système doivent être protégées en conséquence. Ceci vaut en particulier pour le processus d'attribution du numéro d'hôpital au pseudonyme.

Une telle centralisation des projets de recherche présente aussi l'avantage d'accroître la transparence dans le domaine de la recherche au sein d'un hôpital. Les divers hôpitaux présentant une structure distincte et ne mettant pas en œuvre les mêmes ressources matérielles, différentes solutions sont possibles.

1.6 Assurances

1.6.1 Révision totale de la loi sur le contrat d'assurance

Le Conseil fédéral a adopté le message relatif à la révision totale de la loi sur le contrat d'assurance (LCA). Cette révision améliore les dispositions concernant l'information précontractuelle. Une nouveauté est le droit de révocation pour tous les contrats d'assurance. Les dispositions sur les informations relatives à la protection des données ont été reprises mot pour mot. En outre, conformément au projet de révision, les informations précontractuelles devront désormais être remises impérativement à l'assuré avant la déclaration de volonté qui le lie. La majorité de nos commentaires et requêtes ont été pris en compte.

La révision partielle de la loi sur le contrat d'assurance (LCA) avait déjà permis de renforcer les devoirs d'information précontractuelle de l'assureur et d'intégrer les impératifs de la protection des données (voir notre 11e rapport d'activités 2003/2004, ch. 6.2.3). Ainsi, depuis le 1er janvier 2007, l'assureur doit renseigner le preneur d'assurance sur le but et le type de fichier, ainsi que sur les destinataires et sur la conservation des données. Le contenu de cette disposition figure mot pour mot dans le projet de LCA. Cela s'est traduit par une amélioration progressive des dispositions de protection des données dans le domaine de l'assurance (révision partielle de la LCA du 1er janvier 2007 et révision partielle de la LPD du 1er janvier 2008). Cette révision totale permet désormais de réglementer la forme et le moment des informations précontractuelles dans la LCA de manière précise. Désormais, toutes ces informations et ces documents doivent impérativement être communiqués par écrit, de manière compréhensible et en temps utile au preneur d'assurance de manière à ce que celui-ci puisse les consulter avant la déclaration de volonté qui le lie.

Tous nos commentaires sur les devoirs d'information précontractuelle relatifs à la protection des données ont été introduites dans le texte du message. Elles renvoient aux dispositions sur la transparence qui a été renforcée par la révision de la loi sur la protection des données. L'information et la reconnaissabilité sont les deux principales innovations. Outre le devoir d'information relevant du droit des assurances lors de la conclusion du contrat, l'information relevant du droit de la protection des données lors de la collecte des données a désormais un poids plus grand même si l'information expresse n'est prévue dans la LPD que pour les données sensibles et profils de la personnalité. Tant que la collecte de données personnelles normales est reconnaissable,

il n'est pas nécessaire d'informer expressément la personne concernée. Dans les cas individuels, la reconnaissabilité de la collecte est soumise aux principes de la bonne foi et de la proportionnalité. Si l'on tient compte du fait qu'une information adéquate est la condition de la validité des consentements recueillis, il apparaît que l'information doit aussi avoir lieu dans l'intérêt propre de la compagnie d'assurance. La notion de consentement se réfère à cet égard à celle du «consentement éclairé du patient». Dans nos prises de position, nous avons recommandé de se fonder, pour l'élaboration des fiches de protection des données, sur la recommandation du Conseil de l'Europe Rec(2002)9 sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance.

Une autre innovation du projet de LCA est le devoir d'information précontractuelle sur le droit de révocation. Cette information est nécessaire parce que le preneur d'assurance doit désormais avoir le droit de révoquer dans les quinze jours sa demande de conclusion, de modification ou de prolongation du contrat.

Le projet de LCA ne prévoit pas d'inscrire le médecin-conseil dans la loi. En ce qui concerne les données génétiques, la loi fédérale sur l'analyse génétique humaine (LAGH) prévoit déjà expressément le «médecin mandaté». Toutefois la dénomination de médecin-conseil vient du domaine des assurances sociales et est absent de celui des assurances privées. C'est pour cette raison que la notion de médecin mandaté a été choisie pour la LAGH. Les médecins mandatés, les médecins-experts et les médecins-conseils sont tous des médecins qui exercent la même fonction. Ce sont toujours des médecins agissant pour une compagnie d'assurance. La LCA ne contient pas de réglementation permettant à l'assuré, par analogie à l'art. 42 al. 5 de la loi sur l'assurance-maladie (LAMal), de demander que les informations d'ordre médical ne soient fournies qu'au personnel médical. Certes, dans la pratique, les compagnies d'assurance ont déjà un médecin-expert, un service médical ou un médecin-conseil. Malheureusement toutes les personnes impliquées ne le savent pas et il n'est pas toujours clair ni pour les assurés ni pour les médecins que les informations médicales ne doivent être transmises qu'au personnel médical. Pour cette raison, les assurés devraient mentionner expressément dans leur déclaration de consentement qu'ils n'autorisent la communication de leurs données à caractère médical que de médecin à médecin. Les médecins pour leur part ne devraient transmettre les données génétiques conformément à la LAGH qu'au médecin mandaté. Ils ne devraient transmettre les autres données à caractère médical qu'au médecin-conseil ou au service médical de la compagnie d'assurance. La communication de ces données doit se faire dans des enveloppes fermées et adressées à qui de droit.

1.6.2 La fonction de médecin-conseil dans les divers domaines d'assurance

En tant que service de conseil juridique, le PFPDT reçoit régulièrement des demandes concernant des problèmes liés à la protection des données dans le domaine de la santé publique. Un des thèmes qui tient l'affiche est celui de l'engagement de médecins-conseil dans les divers domaines d'assurance.

Depuis la révision du 18 mars 1994 de la loi sur l'assurance-maladie (LAMal), la santé publique connaît une nouvelle institution juridique: le médecin-conseil. Depuis son introduction, cette nouvelle fonction a été à maintes reprises la source de malentendus en ce qui concerne sa position et sa tâche au sein de la santé publique. Nous avons dès le début considéré qu'il était de notre devoir de préciser quelle est la vraie tâche assignée au médecin-conseil par la LAMal. Ainsi, nous avons au cours de l'année passée, lors d'une conférence auprès de la Société suisse des médecins-conseils et médecins d'assurance (SSMC), souligné une nouvelle fois l'importance du médecin-conseil. A notre avis, le médecin-conseil, en tant qu'organe spécial de la loi sur l'assurance-maladie, se trouve confronté aux intérêts conflictuels des assureurs, des fournisseurs de prestations et des assureurs. Indépendant dans ses jugements, il n'est autorisé à transmettre aux organes concernés des assureurs que les informations qui sont nécessaires pour décider de la prise en charge d'une prestation. Le fournisseur de prestations est dans tous les cas fondé ou même, si l'assuré le demande, tenu de ne fournir les indications d'ordre médical qu'au médecin-conseil de l'assureur.

Nous avons également souligné que l'indépendance juridique prescrite par la loi devait tout d'abord résulter dans l'organisation d'un service du médecin-conseil. Ainsi, les locaux réservés aux service du médecin-conseil doivent être suffisamment bien séparés des autres et pouvoir être fermés à clé. Le courrier doit être ouvert uniquement par le personnel du service du médecin-conseil et il doit pouvoir être garanti en tout temps que les données personnelles sensibles ne quittent pas le service du médecin-conseil. Le service doit obligatoirement disposer de son propre réseau de téléphone et de fax. Quant au système informatique, il doit être structuré physiquement de manière à ce que les documents propres au service du médecin-conseil soient archivés exclusivement sur des supports de données propres au service et accessibles uniquement aux collaborateurs du service. Une subordination du médecin-conseil au responsable du service des prestations de l'assureur est à notre avis absolument inconciliable. Le médecin-conseil doit être seul compétent pour le recrutement de son personnel. Nous nous sommes également clairement exprimés dans le sens qu'un

médecin-conseil travaillant pour le compte d'un assureur doit restreindre ses activités au domaine des assurances complémentaires afin d'éviter tout conflit d'intérêt avec d'autres domaines d'assurance (tels que l'indemnité journalière de maladie, la prévoyance professionnelle).

Nous avons également attiré l'attention sur le rôle des médecins dans divers autres secteurs d'assurance. L'«institution» du médecin-conseil n'a de base légale que pour l'assurance de base obligatoire. La LAMal oblige les assureurs-maladie à désigner un médecin-conseil. Dans le domaine de l'assurance-maladie complémentaire, c'est la loi sur le contrat d'assurance (LCA), dans l'assurance-accidents la loi fédérale sur l'assurance-accidents (LAA) qui est applicable. La LCA, la LAA, diverses lois sur les assurances sociales (AI, AVS) ainsi que d'autres branches d'assurance doivent souvent avoir recours pour des usages précis aux connaissances médicales d'un médecin sans qu'elles ne disposent d'une base légale qui leur permette de pouvoir faire appel à un médecin-conseil. Les médecins-conseil des assureurs-maladie, les médecins de la SUVA, du Service médical régional (SMR), du Centre d'observation médicale de l'assurance invalidité (COMAI) ou les médecins experts des assureurs privés ainsi que des entreprises et des autorités se considèrent en première ligne comme médecin et donc comme intermédiaire entre les assureurs, les fournisseurs de prestations et le patient. Dans les milieux juridiques de conseil sur la santé publique, nous avons été confrontés l'année passée à plusieurs reprises à la question de savoir si le rôle du médecin-conseil, tel qu'il est prescrit par la LAMal, ne pouvait pas être transposé de manière analogue dans les autres branches d'assurance (cf. également ch. 1.6.1). Pour autant que les obligations et les droits ainsi que l'indépendance de l'organisation restent garantis, nous n'aurions pas d'objection majeure. Nous sommes cependant de l'avis que des mesures organisationnelles qui garantissent l'indépendance sont bel et bien importantes, mais celles-ci ne suffisent pas à elles seules à protéger les droits des patients dans tous les cas. Le problème se situe d'une part dans la difficulté de définir ce qu'on entend par «données médicales», d'autre part dans l'engagement que prend le médecin-conseil de ne communiquer à l'assureur concerné que les données qui sont absolument nécessaires pour décider si une obligation de fournir la prestation est donnée, un engagement qui laisse pas mal de liberté d'interprétation.

1.6.3 Enquête du PFPDT et de l'OFSP sur la situation en matière de protection des données auprès des assureurs-maladie sociaux reconnus

En collaboration avec l'Office fédéral de la santé publique (OFSP), nous avons – dans le cadre de notre activité de surveillance – effectué une enquête sur la situation en matière de protection des données auprès de tous les assureurs-maladie sociaux reconnus.

Les examens qui ont été effectués auprès de certains assureurs-maladie aussi bien par l'OFSP que par le PFPDT ont révélé des lacunes au niveau de la protection des données. Par la suite les deux organes de surveillance ont à plusieurs reprises invité ces assureurs à se comporter de manière conforme à la législation en matière de protection des données. Dans le cadre de notre activité de surveillance, nous avons au cours de l'exercice précédent mis sur pied avec l'OFSP un groupe de travail et effectué une enquête sur la situation en matière de protection des données auprès des caisses-maladie sociales reconnues. A cet effet, nous avons, encore en décembre 2007, envoyé un questionnaire détaillé avec 70 questions à tous les assureurs-maladie. L'objectif de ce sondage à grande échelle était d'obtenir des explications sur l'organisation en matière de protection des données ainsi que sur son application dans le domaine de l'assurance-maladie.

Après avoir reçu les questionnaires remplis, nous avons été en mesure dans un premier temps de nous faire une image de la situation en matière de protection des données auprès des assureurs-maladie. Nous avons maintenant l'intention, dans un deuxième temps, d'aider les assureurs-maladie à optimiser leur structure d'organisation pour la rendre plus conforme aux exigences de la protection des données.

Finalement, ce sondage va également nous permettre d'émettre des suggestions concernant un audit volontaire en matière de protection des données ainsi que la certification volontaire en matière de protection des données des assureurs-maladie, selon la LPD révisée. Pour améliorer la protection et la sécurité des données, les assureurs-maladie ont la possibilité de faire analyser leurs systèmes, leur procédures et leur organisation par un organe de certification indépendant reconnu; ils n'y sont cependant pas contraints par la loi.

Le dépouillement et l'analyse des questionnaires avec leurs réponses détaillées et les documents joints ont pris beaucoup de temps. Les 93 assureurs-maladie (état à fin 2007) nous ont pour la plupart remis dans les délais des réponses complètes accompagnées de documents. Cette analyse fait l'objet d'un rapport de 50 pages environ et fournit – avec les données générales de surveillance de l'OFSP – une bonne base

pour une optimisation de la protection des données auprès des assureurs-maladie. Nous devons à cet égard rappeler avec insistance que les assureurs-maladie portent seuls la responsabilité de veiller à ce que leurs données ultra-sensibles soient traitées de manière conforme aux exigences de la protection des données et à ce qu'aucun problème au niveau de la sécurité ne survienne. Les deux organes de surveillance sont prêts à soutenir les assureurs-maladie dans cette tâche.

Nous pouvons au préalable déjà mentionner un aspect important de l'analyse, à savoir que la plupart des assureurs-maladie collaborent au sein d'un groupe d'assureurs ou d'une association de caisses-maladie. Ces regroupements doivent être pris en compte lors de l'appréciation des résultats du sondage. Ces derniers ont montré clairement que les assureurs-maladie ne disposent actuellement pas de concepts et d'instruments uniformes pour le respect des exigences de la protection des données.

L'analyse du coeur proprement dit du sondage, à savoir la gestion et l'organisation de la protection des données auprès des assureurs-maladie, a notamment donné les résultats suivants:

59% des caisses-maladie, qui assurent 90% de la population, disposent d'un concept pour la protection des données. Un tel concept informe sur la stratégie à suivre à moyen et long terme au sein de l'entreprise pour mettre en place les mesures permettant de respecter les exigences de la LPD. Il décrit l'organisation de la protection des données qui permet ensuite de définir les tâches concrètes du responsable de la protection des données et des personnes responsables du traitement des fichiers. Le concept de protection des données n'est pas prescrit par la loi.

Seuls 26% des caisses-maladie (qui assurent néanmoins 62% de la population) ont un règlement de traitement pour leurs fichiers de données sensibles. Cela signifie que pour 38% des assurés au moins, aucune directive n'existe concernant la manière de traiter leurs données sensibles. Dans leur cas, ni la protection ni la sécurité des données ne peuvent être garanties. La législation exige cependant que tout fichier soumis à la déclaration obligatoire soit au bénéfice d'un règlement de traitement et que ce dernier soit régulièrement mis à jour. Assurer l'intégralité et l'actualité des règlements de traitement est une des tâches principales du responsable de la protection des données de l'assureur-maladie et sert de base à un traitement conforme à la loi, respectivement à une utilisation conforme à la loi d'un fichier contenant des données personnelles sensibles.

Chez 62% des assureurs-maladie (qui assurent 91% de la population), le responsable de la protection des données dispose d'une formation satisfaisante. Ce qui peut être considéré comme formation satisfaisante dépend du cahier des charges du responsable de la protection des données. Dans les autres cas, le porteur du rôle n'est pas autonome et sujet à un conflit d'intérêts. Chez 40 assureurs-maladie, le responsable de la protection des données n'a pas de cahier des charges écrit décrivant ses tâches.

80% des assureurs-maladie (qui assurent 91% des assurés) ont un responsable de la protection des données. Ce résultat est réjouissant. Les établissements qui n'ont pas de responsable de la protection des données sont tenus de déclarer au PFPDT tous leurs fichiers contenant des données personnelles sensibles et de tenir à jour un règlement de traitement.

Une remarque qui vaut pour tous les résultats est que le score obtenu par les divers assureurs-maladie ne dépend ni de leur taille, ni du fait qu'ils fassent partie d'un groupe ou d'une association. Nous avons au contraire constaté que ce sont justement les petites caisses qui nous ont par exemple présenté des règlements de traitement bons, voire excellents. Malgré les lacunes constatées, il faut néanmoins reconnaître que les assureurs-maladie sont maintenant sensibilisés pour toute cette problématique de la protection des données et qu'ils ont à plusieurs reprises manifesté qu'ils étaient disposés à apporter des améliorations dans ce domaine. Ainsi, une majorité claire a consenti à se soumettre volontairement à un audit régulier de leurs mesures de protection des données. En outre, sachant quel important effort cela implique, quelques assureurs ont aujourd'hui déjà manifesté leur intention de procéder volontairement, en temps opportun, à une certification en matière de protection des données. La certification est toutefois moins bien acceptée qu'un audit. La disposition à se soumettre à un audit ou à une certification ne dépend d'ailleurs pas non plus de la taille de la caisse.

Une description plus détaillée des divers états de fait dépasserait le cadre de ce rapport. Les résultats importants sont ceux qui concernent le contrôle de la rentabilité, le service du médecin-conseil, la gestion des cas (Case management), une procédure qui n'est toujours pas ancrée dans la loi fédérale sur l'assurance-maladie (LAMal), ainsi que la tendance plus forte que prévue des caisses à externaliser, c'est-à-dire à déléguer à des tiers de plus en plus de tâches dans tous les domaines d'activité. Ce point fera l'objet d'un rapport plus détaillé élaboré en commun avec l'OFSP. Dans les mois qui suivent, nous allons en premier lieu continuer à traiter les diverses questions encore en suspens et faire des suggestions aux assureurs-maladie.

1.7 Secteur du travail

1.7.1 Introduction d'un registre des allocations familiales

La nouvelle loi sur les allocations familiales est entrée en vigueur le 1er janvier 2009. Elle prévoit l'introduction d'un registre des allocations familiales. Nous n'avons élevé aucune objection contre le projet de loi.

Le registre des allocations familiales est organisé sur la base des informations concernant l'enfant pour lequel une allocation est perçue. Il permettra de lutter contre les abus, en premier lieu la double perception d'allocations familiales. Pour que le registre des allocations familiales remplisse cette fonction, il faut que toutes les caisses d'allocations familiales livrent régulièrement au registre les données et mutations nécessaires.

Le catalogue de données du registre des allocations familiales ne contiendra probablement pas de données sensibles, ni ne constituera d'une manière générale un profil de la personnalité. Nous avons examiné le projet de loi et n'avons soulevé aucune objection touchant à la protection des données.

1.7.2 Révision de la loi sur l'organisation du gouvernement et de l'administration

L'administration fédérale inscrit actuellement dans la loi la protection des utilisateurs de son infrastructure de télécommunication contre le traitement abusif de données. Cette démarche va de pair avec la création de la base légale permettant à l'administration fédérale de traiter ces données à des fins spécifiques. Nous avons participé à ces travaux législatifs.

Les employés de la Confédération et les tiers qui utilisent l'infrastructure de télécommunication de la Confédération ou qui pénètrent dans des bâtiments administratifs placés sous surveillance vidéo laissent des traces électroniques. Outre les données accessoires produites par la connexion et la déconnexion des communications, des données relatives au contenu peuvent être générées. Dans certains cas, il peut s'agir de données sensibles.

L'enregistrement et le traitement des données résultant de l'utilisation de l'infrastructure électronique de l'administration fédérale ne reposaient jusqu'ici sur aucune base légale formelle. Nous avons recommandé de combler cette lacune dans le cadre de la révision de la loi sur l'organisation du gouvernement et de l'administration (LOGA).

Le projet de révision prévoit que l'administration fédérale pourra en principe enregistrer toutes les données qui résultent de l'utilisation de l'infrastructure électronique. Le traitement des données sera néanmoins restreint par une liste de conditions et par l'énumération exhaustive des buts de traitements admissibles de données. Nous estimons que les organes fédéraux ne doivent être autorisés à traiter les données concernant la connexion et la déconnexion de liaisons électroniques que pour garantir la sécurité de l'information et des services ou contrôler le respect des règlements d'utilisation. A notre avis, l'analyse nominative ne doit avoir lieu qu'en présence d'un soupçon concret d'utilisation abusive de l'infrastructure électronique.

Nous avons participé activement aux travaux d'élaboration du projet de loi. Celui-ci a été envoyé en consultation par le Conseil fédéral au début de l'année 2009.

1.7.3 Révision de la loi sur le personnel fédéral de la Confédération

La révision de la loi fédérale sur le personnel de la Confédération a pour but de créer la base formelle pour le traitement de données personnelles sensibles et de profils de la personnalité dans le système de gestion des données relatives au personnel de l'administration fédérale BV PLUS. La plupart des recommandations que nous avions émises à l'occasion de la première consultation des offices ont été également ignorées dans le nouveau projet de règlement.

Dans le cadre de la première consultation des offices relative à la révision de la loi sur le personnel de la Confédération (LPers), nous avions émis différentes objections concernant la densité normative (cf. notre 15e rapport d'activités 2007/2008, ch. 1.7.4). Lors de la deuxième consultation des offices, nous avons dû constater qu'une large partie de nos objections n'a pas été prise en considération. De même, dans le nouveau projet, notre recommandation concernant les nouvelles tâches de BV PLUS et la procédure d'appel par le portail des utilisateurs E-Gate de données d'évaluation et autres données sensibles n'a rencontré aucun écho. Autre point problématique: tous les autres accès par procédure d'appel qui étaient prévus dans le premier projet de réglementation ont été éliminés du nouveau projet.

La procédure de consultation que le Conseil fédéral ouverte le 19 septembre 2008 a duré trois mois. Selon la planification actuelle, le message relatif à la révision de la LPers sera adopté par le Conseil fédéral durant la première moitié de l'année 2009 et transmis au Parlement.

1.7.4 Les certificats personnels des caisses de pension

Une caisse de pension envoie les certificats personnels de ses assurés à l'employeur, qui distribue ensuite les certificats de caisse de pension à ses employés. Or la caisse de pension n'est pas autorisée à envoyer les certificats à l'employeur. Celui-ci n'a besoin des informations rassemblées sur le certificat de caisse de pension ni du point de vue du droit des assurances, ni du point de vue du droit du travail. Nous considérons la pratique de cette caisse de pension comme non conforme aux dispositions de protection des données, raison pour laquelle nous avons élaboré une recommandation.

Nous avons été informés qu'une caisse de pension envoie les certificats personnels des personnes assurées chez elle à leur employeur, soit à l'adresse que celui-ci a donné à la caisse de pension. Les certificats de caisse de pension sont ensuite transmis par voie interne aux employés. Les certificats n'étant pas adressés personnellement, l'employeur peut prendre connaissance de leur contenu avant de les distribuer.

De notre point de vue, la manière dont cette caisse de pension procède actuellement à l'envoi des certificats n'est pas conforme à la protection des données. Les informations figurant sur les certificats de la caisse de pension ne sont destinées qu'aux assurés. L'employeur n'en a besoin ni sous l'angle du droit des assurances, ni sous l'angle du droit du travail. La caisse de pension doit organiser l'envoi de ces certificats de sorte que l'employeur ne puisse y avoir accès.

Nous avons pris contact avec la caisse de pension et l'avons priée de prendre position à cet égard. Elle a invoqué tout d'abord des motifs d'ordre organisationnel pour justifier cette pratique. Nous lui avons ensuite soumis des propositions visant à résoudre de manière pragmatique ce problème d'organisation. La caisse de pension n'a toutefois pas suivi nos propositions en avançant que l'employeur avait besoin de consulter ces données pour des motifs relevant du droit des assurances et du droit du travail. Nous lui avons répondu que la caisse de pension ne possédait aucun motif justificatif l'autorisant à remettre les certificats à l'employeur et que l'employeur n'avait besoin de ces données ni pour la mise en œuvre de la loi sur la prévoyance professionnelle ni pour l'exécution du contrat de travail et enfin que cette pratique enfreignait les règles de protection des données.

L'échange de lettres n'a pas permis d'aboutir à une solution. Nous allons émettre une recommandation à l'adresse de cette caisse de pension.

1.7.5 Questionnaire relatif à l'admission dans une caisse de pension

Ce n'est que dans le domaine de l'assurance surobligatoire que des données relatives à la santé peuvent être prélevées au moment de l'admission dans une caisse de pension. S'agissant de l'admission dans l'assurance obligatoire, la caisse de pension n'est pas autorisée à demander ce genre d'informations puisqu'il existe un devoir légal d'admission.

Il s'agissait ici d'examiner si les caisses de pension étaient habilitées à recueillir, sur la base d'un questionnaire, des données relatives à la santé des personnes effectuant une demande d'admission. Le questionnaire ne permettait pas clairement de déterminer s'il s'agissait d'une assurance obligatoire ou d'une assurance surobligatoire selon la loi sur la prévoyance professionnelle vieillesse survivants et invalidité (LPP).

Dans notre prise de position, nous avons souligné la grande différence entre l'assurance obligatoire et l'assurance surobligatoire selon la LPP. Dans le domaine de l'assurance obligatoire, il n'est pas permis de recueillir des données relatives à la santé car la caisse de pension est légalement tenue d'accepter la personne. Par conséquent, quel que soit leur état de santé, les personnes demandant à entrer dans une caisse de pension doivent être admises, dans la mesure où les conditions de la LPP sont remplies.

Par contre, il est possible de demander des données relatives à la santé en vue de l'admission dans une assurance surobligatoire selon la LPP. Dans ce cas, pour les risques décès et invalidité, les assureurs peuvent émettre des réserves pour des raisons de santé; c'est pourquoi une évaluation des risques concernant la santé joue un grand rôle dans la procédure d'admission. La personne qui désire conclure une assurance surobligatoire doit, avant son admission, informer la caisse de pension des faits qui pourraient influencer la décision de l'assureur. De son côté, l'assurance doit informer la personne qui fait la demande d'adhésion du but dans lequel les données relatives à la santé sont prélevées. Les données relatives à la santé qui peuvent être collectées en vue d'une évaluation des risques relèvent de la proportionnalité. Seules les données nécessaires à la réalisation du but fixé peuvent être collectées. Selon le principe de la bonne foi, il se peut que la personne ayant déposé la demande doive fournir des informations supplémentaires. Au besoin, il convient de l'informer si la réponse aux questions posées est obligatoire ou facultative et quelles peuvent être les conséquences pour la personne concernée si elle refuse de donner le renseignement demandé.

1.7.6 Système de gestion des données relatives au personnel de l'administration fédérale

L'examen du système de gestion des données relative au personnel de l'administration fédérale BV PLUS n'a pas fait ressortir de problèmes majeurs, que ce soit à l'Office fédéral du personnel, responsable du système, ou au Service du personnel de la Chancellerie fédérale en tant qu'utilisateur final. Placé sous la responsabilité de l'Office fédéral de l'Informatique, cet examen n'est pas encore terminé.

Fin 2007, en notre qualité d'autorité de surveillance de la protection des données, nous avons examiné auprès des services responsables du système de traitement des données BV PLUS ainsi qu'auprès d'un utilisateur final de ce même système si son application avait lieu dans le respect des dispositions en matière de protection des données. Les services contrôlés, étaient l'Office fédéral du personnel (OFPER) et l'Office fédéral de l'informatique et de la technologie (OFIT) en tant que responsables du système, ainsi que le Service du personnel de la Chancellerie fédérale en tant qu'utilisateur final. Le contrôle a porté sur deux thèmes, à savoir la sécurité des données et le catalogue de données.

Les contrôles effectués auprès de l'utilisateur final n'ont pas soulevé de problèmes notables, ce qui a permis de clore les travaux de manière rapide et sur une note positive.

A l'OFPER, il s'agissait de savoir si les collaborateurs donnent leur consentement à l'exécution, par BV PLUS, des paiements de cotisations de membres aux associations concernées. Selon les informations données par l'OFPER les collaborateurs donnent aux associations leur accord écrit, au moment de leur adhésion, pour que celle-ci soit communiquée au service du personnel de leur unité administrative. Or celui-ci ne reçoit pas les copies des déclarations de consentement de la part des associations. Nous avons donc enjoint l'OFPER de recommander aux départements d'exiger ces copies.

A l'OFIT, nous avons constaté que l'on pouvait procéder à des améliorations dans différents domaines. Pour ce qui est de l'organisation, nous avons remarqué que le règlement de traitement établi il y a des années n'a guère été actualisé. Il manque en outre un expert SAP en matière de sécurité des données et de l'information. Nous avons suggéré de transmettre sous forme cryptée à l'administration fiscale du canton de Berne les données concernant les salaires des employés de la Confédération imposables à Berne. De plus, nous avons recommandé à l'OFIT de consigner par écrit et de soumettre à une évaluation périodique les télé(dé)chargements (uploads et downloads) de données de l'ordinateur central vers l'ordinateur du poste de travail d'une part et les accès d'utilisateurs bénéficiant de privilèges sur le système d'autre part. Nous avons donc conseillé à l'OFIT de procéder aux améliorations nécessaires.

1.8 Economie et commerce

1.8.1 Révision du droit des poursuites et faillites

Nous estimons que l'inscription de données sur l'extrait du registre des poursuites est actuellement réglementée de manière trop peu différenciée. Nous avons donc proposé, dans le cadre de la consultation des offices en vue de la révision de la loi sur la poursuite pour dettes et faillites (procédure d'assainissement), de modifier les délais d'inscription. A notre avis, un échelonnement de ceux-ci répond mieux aux exigences de la protection des données et peut inciter la personne concernée à régler plus rapidement ses factures impayées.

Conformément à la réglementation légale actuelle, l'extrait du registre des poursuites fournit des données en matière de poursuite pendant une période de cinq ans. Il n'existe que trois exceptions où aucun renseignement n'est donné, à savoir: a. lorsque la poursuite est nulle et non avenue ou a été levée sur la base d'un recours ou d'un jugement; b. lorsque le débiteur a obtenu gain de cause sur la base d'une action en répétition de l'indu, ou encore c. lorsque le créancier a retiré la poursuite. Dans la pratique actuelle, même les poursuites qui ne sont pas maintenues (soit un bon tiers de toutes les poursuites qui sont engagées) sont mentionnées dans l'extrait du registre des poursuites. Il en va de même des poursuites réglées en bonne et due forme (qui sont néanmoins accompagnées de la mention «liquidé»). Du fait du caractère relativement sensible des données du registre des poursuites, une réglementation si peu différenciée apparaît inadéquate ainsi que disproportionnée du point de vue du droit de la protection des données. Dans la pratique, de nombreux cantons ne renseignent plus aujourd'hui que sur les trois dernières années, sauf si souhaité. D'un côté cela semble insuffisant (par exemple en cas de poursuite en réalisation d'un gage immobilier accompagnée d'un contentieux juridique, la poursuite encore en cours n'est souvent plus indiquée) et d'un autre côté cela semble aller trop loin (par exemple on ne voit pas pourquoi des poursuites liquidées devraient demeurer mentionnées dans le registre des poursuites durant cinq ans).

En vue de mettre en place un droit de consultation échelonné dans le temps, nous proposons que l'art. 8a al. 4 LP soit modifié comme suit: «Le droit de consultation de tiers s'éteint un an après la clôture de la procédure lorsque la poursuite a été liquidée conformément à l'art. 12 al. 2 LP. Il s'éteint trois ans après la clôture de la procédure lorsque la poursuite n'a pas été continuée conformément à l'art. 88 LP. Dans tous les

autres cas, le droit de consultation de tiers s'éteint après clôture de la procédure. Les autorités judiciaires et administratives peuvent continuer à demander des extraits si une procédure est pendante auprès d'elles».

La réputation financière d'une personne dans le monde des affaires joue un rôle qu'il ne faut pas sous-estimer. Cette réputation financière est d'autant plus importante que la diffusion des renseignements en matière de crédit ne cesse de s'élargir. Les informations deviennent d'autant plus sensibles que le comportement en matière de paiement des personnes concernées est de plus en plus transparent.

Cette nouvelle réglementation rétablirait après un an la réputation des débiteurs qui ont payé leur dette. En revanche, les poursuites infructueuses resteraient mentionnées dans le registre des poursuites durant cinq années complètes. D'un côté, cette réglementation tient mieux compte des circonstances actuelles et de l'autre elle est tout à fait susceptible d'inciter le débiteur à s'acquitter plus rapidement de ses obligations dans l'intérêt de sa réputation financière.

1.8.2 Publications privées de données du registre du commerce

La publication sur Internet de données du registre du commerce par des entreprises privées renforce l'effet de notoriété de ce même registre et a donc été jugée comme conforme au droit par le Tribunal fédéral administratif. Nous sommes toutefois d'avis que l'effet de notoriété ne doit pas être assimilé à un effet maximal de publicité. Nous demandons donc aux fournisseurs privés de données du registre du commerce de prendre les mesures permettant de mener à une publicité moindre.

Dans son arrêt du 26 février 2008, le Tribunal administratif fédéral approuve le traitement et l'enregistrement illimité de données du registre du commerce par des fournisseurs privés. L'intérêt de la diffusion publique d'informations du registre du commerce subsisterait sans limitation temporelle, indépendamment du fait que la source de données soit publique ou privée, aussi longtemps que les données ne sont pas modifiées quant au fond.

Malgré ce jugement, l'un des plus grands fournisseurs privés d'informations du registre du commerce sur Internet en Suisse a concrétisé volontairement quelques-unes de nos requêtes. Ainsi, il n'est pratiquement plus possible de chercher des personnes ou des entreprises qui ont été effacées sans entrer un nom d'utilisateur dans le système (Login).

Pourtant, de nombreuses personnes sont toujours dérangées par le fait que lors de recherches sur Internet à partir du nom de personnes physiques ou d'entreprises, des informations du registre du commerce émanant de sociétés de renseignements commerciaux apparaissent au premier plan alors qu'elles ne sont plus actuelles. Dans le cas de faillites notamment, les personnes concernées ont véritablement intérêt à ce que ces données ne figurent pas en première page des résultats du moteur de recherche.

Nous reconnaissons l'effet de notoriété du registre du commerce qui est inscrit dans le droit des obligations. Destiné à faciliter les échanges économiques, un registre du commerce aisément et librement accessible à tous atteint son objectif dans sa forme actuelle. Néanmoins, de l'avis du PFPDT, la publicité du registre ne doit pas équivaloir à une publicité maximale.

Les fournisseurs privés d'informations du registre du commerce ont tout intérêt à ce que leurs sites web soient visités le plus souvent possible afin de générer des rentrées publicitaires. La majorité d'entre eux optimisent donc leurs sites de manière à ce qu'ils apparaissent le plus souvent possible dans les résultats des moteurs de recherche. Ainsi, lorsque l'on recherche une entreprise à l'aide d'un moteur de recherche, les résultats apparaissant au premier plan sont les inscriptions du registre du commerce la concernant. De notre point de vue, cet effet de publicité maximale ne relève plus du but du registre du commerce et constitue de ce fait un traitement illicite de données. Pour cette raison, nous souhaitons reprendre ce thème durant l'année en cours dans le but de mieux protéger la personnalité des personnes concernées sans restreindre l'effet de notoriété du registre du commerce.

1.8.3 Droit d'accès et d'effacement auprès de sociétés commerciales

Suite à de nombreuses plaintes, nous sommes intervenus auprès de certaines sociétés commerciales – notamment de vente par correspondance – afin de les rendre attentives à leur devoir de respecter la LPD, et tout particulièrement de garantir le droit d'accès et d'effacement aux personnes qui en font la demande.

Selon la LPD, les sociétés commerciales ne peuvent traiter des données contre la volonté expresse de la personne concernée et en particulier elles ne peuvent pas adresser de courrier publicitaire si les personnes ont expressément refusé. La personne concernée peut ainsi à tout moment demander l'effacement de ses données personnelles à des fins de marketing. L'utilisation de l'adresse à des fins publicitaires peut également être soumise d'emblée à une interdiction générale (p. ex. par le biais

d'une astérisque dans l'annuaire téléphonique ou de l'inscription dans la liste Robinson) ou être l'objet, ultérieurement, d'une interdiction particulière; c'est le cas notamment lorsque le destinataire d'un courrier renvoie l'envoi commercial à l'expéditeur avec une mention spéciale.

De plus, la LPD oblige tout maître de fichier de communiquer à toute personne qui le requiert toutes les données personnelles la concernant, le but et le cas échéant la base juridique du traitement, les catégories de données personnelles traitées, de participants au fichier et de destinataires des données. Cette procédure est en règle générale gratuite.

Nous avons écrit à diverses sociétés afin de les rendre attentives à leurs devoirs légaux d'effacer, sur requête des personnes concernées, et de répondre conformément à la loi aux demandes d'accès. En outre, nous attiré l'attention des entreprises en question sur le fait que les personnes concernées avaient, le cas échéant, la possibilité de faire valoir leurs droits auprès d'un juge. Dans certains cas particuliers, nous avons également la possibilité d'élaborer l'état de faits et d'émettre des recommandations aux sociétés ne respectant pas ces droits.

1.8.4 Recommandation en matière de contrôle des locataires

Au cours de l'année 2008, nous avons procédé à un examen des faits auprès d'une société de renseignements économiques. La société en question offre depuis peu un service permettant aux bailleurs de vérifier les données concernant les locataires et de réduire le risque de pertes de loyers. Nous avons constaté des lacunes au niveau de la pertinence en matière de solvabilité des données offertes ainsi que de la garantie du droit à l'information et du droit à l'effacement des données. Nous avons donc émis une recommandation.

Sous le nom de «Mietercheck» (contrôle des locataires), une société de renseignements économiques offre une nouvelle prestation de services permettant aux bailleurs de se procurer en ligne des renseignements sur des locataires potentiels, l'objectif étant de vérifier les données concernant ces personnes et, partant, d'éviter des pertes de loyer.

Dans le but d'estimer la solvabilité de locataires potentiels, le service «Mietercheck» utilisait un système de classement (score) qui intégrait non seulement les données des personnes concernées, mais aussi celles de leur entourage. «Mietercheck» évaluait alors les personnes concernées en utilisant un système de feux de signalisation et donnait aux bailleurs des instructions quant à la conclusion du contrat.

Une personne concernée nous a signalé l'existence de cette prestation et nous avons donc immédiatement contacté la société en question. À la même période, le traitement des données effectuées par la société de renseignements a suscité l'attention des médias.

Comme l'a montré l'examen des faits, la société a procédé entre-temps à quelques modifications de ses services. En particulier le système de classement (score) et les données socioculturelles ont été supprimés. Notre examen a néanmoins montré que le traitement des données n'était pas conforme à la protection des données, raison pour laquelle nous avons émis plusieurs recommandations.

En premier lieu, la société devra évaluer les antécédents de paiement de manière plus transparente. En effet, la personne concernée est dans l'incapacité de reconnaître comment ses antécédents de paiement sont classés, ni de voir qu'en plus, «Mietercheck» les évalue sur la base de son système de feux de signalisation.

Deuxièmement, l'évaluation de la solvabilité d'une personne sur la base de ses relations avec une entreprise doit être limitée aux cas qui influent effectivement sur la solvabilité de la personne concernée. En effet, toutes les relations d'une personne avec une entreprise ne sont pas nécessairement pertinentes en matière de solvabilité.

Troisièmement, ces mises en relation doivent être reconnaissables pour la personne concernée et les clients. Nous estimons enfin qu'il est disproportionné de mettre en relation d'une manière générale les données concernant des personnes physiques et les données concernant des entreprises.

Quatrièmement, nous estimons que l'entreprise ne doit plus lister toutes les adresses connues d'une personne pour calculer sa durée moyenne d'habitation. En effet, la durée d'un bail peut dépendre de facteurs qui n'ont aucun rapport avec de quelconques difficultés de paiement comme la profession du locataire ou des membres de sa famille, son cadre de vie, l'offre de logements, etc. Si la durée d'habitation moyenne ne constitue pas une donnée pertinente quant à la solvabilité, elle ne permet pas davantage de conclure que le locataire est un «nomade» en puissance. Par ailleurs, nous avons souligné que les données sur le changement de domicile sur plusieurs années doivent être considérées comme un profil de la personnalité.

Cinquièmement, nous avons demandé que les données sur la solvabilité des personnes qui partagent le même ménage que le locataire potentiel soient supprimées. Nous considérons en effet qu'il est disproportionné de mettre en relation les données de solvabilité de toutes les personnes vivant dans le ménage avec les données de la personne au sujet de laquelle on désire obtenir des renseignements. D'une part, les don-

nées des colocataires ne sont pertinentes que si sont parties au nouveau contrat de loyer. D'autre part, les données sur la solvabilité de personnes vivant sous le même toit ne permettent en principe pas de tirer des conclusions sur la solvabilité du locataire potentiel. Par ailleurs, ce dernier n'est pas en mesure de reconnaître que le fichier met en relation ses données avec celles des personnes vivant dans le même ménage.

La sixième recommandation que nous avons émise concerne l'accès au fichier. Nous avons demandé que cet accès ne soit octroyé qu'en fonction de la finalité poursuivie, c'est-à-dire uniquement à des bailleurs professionnels. Si par exemple une assurance-dépôt de garantie n'est pas elle-même bailleur professionnel, la société de renseignements économiques ne doit lui fournir que les informations pertinentes sur la solvabilité dont l'assurance a besoin pour la conclusion ou l'exécution de ses contrats.

Les possibilités actuelles de consultation fournissent plus de données qu'il n'en faut. Nous avons donc recommandé à la société de renseignements de restreindre d'un point de vue technique la consultation de telle manière que ses clients puissent introduire d'autres critères par étape, selon le nombre de résultats.

Enfin, nous avons enjoint à la même société de remettre aux personnes qui font valoir leur droit d'accès toutes les informations les concernant. Par l'intermédiaire du service «Mietercheck», les bailleurs peuvent consulter des données qui ne sont actuellement pas communiquées aux personnes directement concernées. Parmi ces données se trouvent également des informations qui sont seulement mises en relation ou sont calculées systématiquement à partir des ensembles de données. La personne concernée ne peut voir quelles données la société traite effectivement et ne peut donc pas faire valoir correctement son droit à la rectification et à l'effacement des données.

Notre recommandation figure en annexe, au ch. 4.1.6. La société de renseignements a pris position. Il n'est à ce jour pas encore clair si le cas sera porté auprès du Tribunal administratif fédéral.

1.8.5 Communication de données personnelles à des tiers par des associations et des organisateurs de manifestations sportives.

Les associations ou les organisateurs d'une manifestation ne peuvent sans autre communiquer à leurs sponsors ou à d'autres tiers les adresses de leurs membres ou des participants. Une communication de données personnelles à des fins de marketing ne peut être justifiée que par le consentement libre et éclairé des personnes concernées. Nous avons rendu les personnes responsables attentives aux conditions légales d'un traitement de données et leur avons recommandé d'adapter leurs statuts et leurs règlements en conséquence.

Cette année, nous avons reçu de nombreuses plaintes de la part de membres d'association ainsi que de la part de participants à des manifestations sportives concernant la communication de leurs adresses à des tiers à des fins de marketing (sponsors, caisses-maladie). Les personnes concernées n'ont pas – ou insuffisamment – été informées et n'ont pas eu la possibilité de s'opposer à une telle communication. Suite à certains articles parus dans la presse à ce sujet, nous avons en outre reçu de nombreuses questions de la part d'associations ou d'organisateurs de manifestations sportives. Nous avons informé les personnes concernées et les responsables de la situation légale dans ce domaine ainsi que de leurs droits, respectivement de leurs devoirs.

L'utilisation des données personnelles des membres d'une association ou celle des participants d'une manifestation sportive est soumise à la loi sur la protection des données. Un traitement de données personnelles doit se fonder sur un motif justificatif et respecter les principes généraux de la LPD. La communication des données ainsi que ses finalités doivent en particulier être reconnaissables pour les personnes concernées. La communication ne peut être effectuée contre leur volonté expresse sans un motif justificatif. Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances.

En ce qui concerne le traitement des données des participants d'une manifestation sportive, les personnes s'inscrivant à une manifestation sportive peuvent en règle générale s'attendre à ce que les données transmises dans le cadre de l'inscription soient utilisées pour des fins directement liées au bon déroulement de la manifestation, soit pour l'envoi d'informations relatives à l'organisation de la course, l'attribution d'un numéro de dossard, le chronométrage, le classement, etc. Le traitement des données peut alors être sans autre déduit des circonstances et est donc reconnais-

sable; une information particulière à cet égard n'est par conséquent en principe pas nécessaire. Le traitement des données personnelles pour des finalités directement liées à l'organisation de la course est en principe justifié par le consentement implicite des participants.

En revanche, la communication de données personnelles à un photographe particulier, à des sponsors ou à d'autres tiers ne ressort pas des circonstances et nécessite donc une information spécifique. Seul le consentement des personnes concernées peut justifier une communication de données à des tiers à des fins de marketing. Le consentement n'est valable que si la personne concernée exprime sa volonté librement et après avoir été dûment informée. Les personnes concernées doivent avoir la possibilité de refuser que l'on transmette leurs adresses à des tiers.

Il convient d'informer les personnes concernées – au plus tard lors de l'inscription – sur la communication de leurs données personnelles à des tiers, sur l'identité de ceux-ci et sur la finalité de la communication (p. ex. publicité). De plus, il convient de leur donner la possibilité de s'opposer cette transmission de données. La mention d'une communication à des tiers doit être bien visible pour les personnes concernées; une simple mention tout au fond du règlement de participation et sans possibilité de refus n'est pas conforme aux principes de la protection des données.

Nous avons recommandé aux organisateurs de manifestations sportives de prévoir dans le bulletin d'inscription de la manifestation une case à cocher: «oui, je consens à ce que mes données personnelles soient transmises aux sponsors à des fins de marketing» et de préciser l'identité des sponsors dans le règlement de la manifestation.

S'agissant de l'utilisation des données personnelles des membres d'une association, la liste des adresses des membres d'une association ne peut être transmise à des tiers à des fins de marketing que dans la mesure où une telle communication est reconnaissable et que les personnes concernées ont donné leur consentement, ou n'ont pas manifesté leur désaccord.

Nous recommandons généralement aux associations de prévoir ce genre de communication dans leurs statuts, au moment de l'adhésion ou encore par un courrier spécifique. Les personnes concernées doivent en outre être informées de leur possibilité de s'opposer en tout temps à une telle utilisation de leurs données personnelles à des fins de marketing.

Des informations détaillées sur ce thème se trouvent dans notre fiche thématique intitulée «Aide-mémoire concernant l'utilisation des données personnelles des membres d'une association». Celle-ci est disponible sur notre site web www.leprepose.ch sous la rubrique Documentation – protection des données – feuillets thématiques.

1.9 International

1.9.1 Mise en œuvre Schengen: La protection des données au niveau fédéral

Après avoir collaboré à l'évaluation de protection des données effectuée par l'Union européenne, nous avons commencé à développer nos activités de surveillance et d'information dans le cadre de Schengen. Nous avons mis en place un groupe de coordination avec les autorités cantonales de protection des données. Nous avons procédé à un contrôle auprès d'une représentation diplomatique suisse à l'étranger et publié des documents d'information sur notre site web.

Avant que la coopération instaurée par l'Accord d'association à Schengen (entré en vigueur en mars 2008) ne devienne opérationnelle pour la Suisse, nous avons participé à l'évaluation de la capacité de la Suisse à mettre en œuvre l'Acquis de Schengen. En juin 2008, l'Union Européenne a estimé que, globalement, les exigences en matière de protection des données découlant de la coopération Schengen étaient remplies en Suisse. Ainsi, la participation de la Suisse au Système d'Information Schengen (SIS) est devenue effective.

Toutefois, l'Union Européenne a adressé des recommandations à la Suisse. Celles-ci concernaient notamment l'indépendance des autorités de protection des données, la coopération entre ces dernières, leurs ressources, leurs activités de contrôle ainsi que la sensibilisation des utilisateurs du SIS et l'information du public. Le comité d'experts a en particulier insisté sur la nécessité d'augmenter l'indépendance du PFPDT ainsi que ses ressources budgétaires et en personnel afin qu'il soit en mesure de remplir les nouvelles tâches qui lui sont dévolues dans ce contexte.

En collaboration avec divers offices fédéraux, nous avons participé à la mise en œuvre de plusieurs des mesures préconisées. Pour l'essentiel, le Conseil fédéral a décidé de nous attribuer trois nouveaux postes de travail à partir de l'année 2010. Dans le cadre du projet de révision de la loi fédérale sur le personnel, il est prévu de nommer le préposé pour une période de fonction de quatre ans; ceci doit permettre de garantir une plus grande indépendance institutionnelle du PFPDT. D'autres mesures sont en discussion, comme la nomination du préposé par le Conseil fédéral avec ratification du Parlement ainsi que le mode de fonctionnement budgétaire du service.

Après avoir collaboré à l'évaluation effectuée par l'Union européenne, nous avons mis en place diverses activités de contrôle des traitements de données, d'information des utilisateurs du SIS et de sensibilisation de l'opinion publique. Afin de garantir une surveillance efficace et effective, nous avons en particulier développé la collaboration avec les autorités cantonales de protection des données qui sont également compétentes pour la surveillance des utilisateurs cantonaux du SIS. Un groupe de coordination des autorités suisses de protection des données, que nous présidons, sert désormais de plateforme de coordination pour les activités de contrôle et d'information desdites autorités dans le domaine de la coopération Schengen/Dublin.

Sur la base des expériences récoltées lors de notre premier contrôle auprès de la représentation diplomatique suisse en Ukraine (voir ch. 1.9.2), nous allons poursuivre et développer nos activités de surveillance. Ainsi, des inspections vont être planifiées et mises en place auprès d'organes fédéraux traitant de données dans le cadre du SIS, tels que l'Office fédéral de la police, l'Office fédéral des migrations et des représentations diplomatiques suisses à l'étranger.

Enfin, nous avons non seulement la compétence de surveiller le SIS et les services impliqués dans la gestion et l'utilisation du système, mais également la tâche de veiller à garantir l'exercice effectif des droits des personnes concernées par des traitements de données personnelles. Ainsi, nous avons élaboré et publié sur notre site web une feuille d'information relative aux droits des personnes concernées par des traitements de leurs données personnelles dans le SIS.

1.9.2 Mise en œuvre Schengen: Contrôle du PFPDT auprès de la représentation diplomatique suisse en Ukraine

En notre qualité d'autorité de surveillance des organes fédéraux autorisés à utiliser le système d'information Schengen (SIS), nous avons procédé à un contrôle auprès de la représentation diplomatique suisse en Ukraine à Kiev. Celui-ci avait pour objet les processus de traitement de données personnelles dans la procédure d'établissement des visas et autres titres de séjour en vue de l'entrée de ressortissants d'Etats tiers dans l'espace Schengen via la Suisse. Les recommandations que nous avons émises concernaient principalement la formation du personnel appelé à utiliser le SIS, la protection et la sécurité technique des traitements de données personnelles, les contrats d'externalisation de prestations et l'exercice des droits des personnes concernées. Actuellement, nous suivons la mise en œuvre des recommandations en collaboration avec le DFAE et l'Office fédéral des migrations.

En tant qu'autorité de surveillance des organes fédéraux en matière de protection des données, nous sommes chargés de contrôler les traitements de données personnelles du système d'information Schengen (SIS), en particulier les traitements effectués par les organes fédéraux autorisés à utiliser le SIS, ce, conformément aux exigences requises par la coopération Schengen. Nous effectuons, entre autres, des contrôles en matière de protection de données auprès des représentations diplomatiques et consulaires suisses à l'étranger. Ces inspections portent sur les processus de traitement de données personnelles dans la procédure d'établissement des visas et autres titres de séjour en vue de l'entrée de ressortissants d'Etats tiers dans l'espace Schengen. Cette procédure implique l'utilisation du SIS par le personnel des représentations suisses.

Dans ce contexte, nous avons procédé, de mai à octobre 2008, à un contrôle auprès de la représentation diplomatique suisse en Ukraine à Kiev. Sur la base de nos constatations, nous avons rendu nos conclusions dans un rapport et adressé des propositions d'amélioration ainsi que des recommandations au Département fédéral des affaires étrangères (DFAE). Celles-ci concernaient principalement la formation du personnel devant utiliser le SIS, la protection et la sécurité technique des traitements de données personnelles, les contrats d'externalisation de prestations de traitements de données personnelles ainsi que l'effectivité des droits des personnes concernées par des traitements de données personnelles.

Nous avons en particulier rappelé la nécessité, dans le cadre de la mise en oeuvre de la coopération Schengen, d'une formation spécifique du personnel des autorités disposant d'un accès au SIS. Avant d'être autorisé à traiter des données conservées dans le SIS, ce personnel doit en effet recevoir une formation appropriée concernant les règles en matière de sécurité et de protection des données et être informé des infractions et sanctions pénales en la matière.

Nous avons recommandé de renforcer la protection des traitements de données personnelles, en particulier de la communication des données transmises des représentations suisses aux autorités suisses et aux personnes privées, notamment la sécurité technique lors de la communication des données par le biais d'un dispositif sécurisé de cryptage.

Par ailleurs, nous avons demandé à ce que les représentations suisses prévoient, dans leurs contrats d'externalisation de prestations conclus avec des entreprises extérieures mandatées pour certains traitements de données personnelles, des clauses relatives à la sécurité et à la protection de ces données (p. ex. concernant les finalités et la confidentialité des traitements de données, la sécurité technique des données, comme la communication au moyen d'un dispositif sécurisé de cryptage, la protection contre des traitements indus, la conservation et l'effacement des données, etc.).

Enfin, afin de garantir l'effectivité des droits des personnes concernées par des traitements de données personnelles, nous avons recommandé que le personnel diplomatique et consulaire soit correctement informé des procédures légales relatives à l'exercice des droits des personnes concernées par des traitements de données.

Actuellement, nous coordonnons la mise en œuvre des propositions d'amélioration et des recommandations en collaboration avec le DFAE ainsi que l'Office fédéral des migrations, également concerné par certaines des mesures.

1.9.3 Coopération internationale

Les données personnelles ne s'arrêtent pas aux frontières nationales. Il est dès lors primordial pour assurer l'effectivité de la protection des données que les autorités nationales de protection des données collaborent entre elles et soient également actives sur la scène internationale. Nous participons ainsi en particulier aux travaux du Conseil de l'Europe, de la Conférence européenne et de la Conférence internationale des commissaires à la protection des données, des instances de contrôle communes Schengen et Eurodac et de l'Association francophone des autorités de protection des données.

Conseil de l'Europe

Nous avons pris part aux travaux du comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD, Convention 108) et de son bureau. Le comité a poursuivi ses réflexions relatives au droit fondamental à la protection des données qui pourrait être inscrit dans un instrument juridique contraignant (par exemple le protocole additionnel à la Convention européenne des droits de l'homme). Bien qu'une majorité du comité soit favorable à un tel instrument, le comité a décidé de suspendre momentanément les discussions et d'attendre notamment l'entrée en vigueur du traité de Lisbonne qui consacre ce droit fondamental et qui prévoit l'adhésion des instances européennes à la Convention européenne des droits de l'homme. Le comité, respectivement son bureau, a entamé des travaux en vue de l'élaboration d'une recommandation sur la protection des données à caractère personnel utilisées dans le cadre du profilage. Les outils informatiques et les technologies de l'information permettent en effet, à partir de la collecte de données, de créer des mécanismes de catégorisation des individus, de déduire ainsi des données personnelles et de traiter des données relatives aux interactions des individus avec leur environnement physique ou numérique. Ces techniques permettent notamment l'enregistrement des comportements et des émotions des personnes et en facilitent l'interprétation. Le profilage est ainsi susceptible de porter gravement atteinte à la dignité de la personne, à ses droits et libertés fondamentales, y compris ses droits économiques et sociaux. Le comité est d'avis qu'il faut fixer des règles afin d'encadrer les activités de profilage. Enfin, le comité a appelé le comité des Ministres à promouvoir la Convention 108 et son protocole additionnel, notamment en invitant des Etats tiers à adhérer à ses instruments, comme le permet la Convention. L'adhésion d'Etats tiers constituerait un premier pas vers un instrument universel en matière de protection des données.

Conférence européenne des commissaires à la protection des données

La Conférence européenne des commissaires à la protection des données s'est tenue à Rome du 17 au 18 avril 2008 sur l'invitation de l'autorité italienne de protection des données. La conférence est un lieu d'échange entre autorités européennes de protection des données autour des sujets d'actualité. En particulier, la Conférence a débattu des enjeux pour la vie privée eu égard aux politiques de sécurité, aux besoins de l'économie et aux développements technologiques. La conférence a en outre adopté les règles de fonctionnement de son groupe de travail sur la police et la justice et adopté une résolution concernant les contrôles des personnes entrant ou sortant de l'espace Schengen. Cette résolution appelle les autorités compétentes à évaluer l'effectivité et l'efficacité des mesures existantes avant d'envisager un renforcement des mesures portant atteinte aux droits et libertés fondamentales des individus. Elle demande que la nécessité et la proportionnalité de nouvelles mesures soient préalablement démontrées. Intervenant dans le cadre d'une table ronde consacrée à la vie privée et à la sécurité, nous avons attiré l'attention de la Conférence sur le risque croissant de déséquilibre au détriment des droits et des libertés fondamentales résultant des politiques de sécurité, sans pour autant que l'objectif de sécurité ne soit nécessairement atteint. Si un niveau suffisant de sécurité est une condition de la protection effective des droits humains, il convient de redimensionner l'importance des mesures à mettre en place et de rappeler que la sécurité passe par le respect des droits et des libertés de chaque individu. Sans protection des données, la sécurité et la démocratie pourraient laisser place à un Etat de méfiance, de violence et de répression. Il est ainsi indispensable de procéder à une véritable analyse de l'efficacité et de l'efficience des mesures déjà mises en place et de procéder à une étude d'impact avant de proposer de nouvelles restrictions aux droits et libertés fondamentales. Dans ce cadre les autorités de protection des données doivent intensifier leur collaboration et adopter des positions communes harmonisées. Elles doivent accentuer leur politique d'information, de communication et de sensibilisation. Elles doivent être impliquées dans le processus qui conduit à l'adoption éventuelle de mesures restreignant les droits des individus.

Groupe de travail «Police et Justice»

Nous participons régulièrement aux travaux du Groupe de travail «Police et Justice» de la Conférence européenne des commissaires à la protection des données. Ce groupe a pour mission de suivre les développements législatifs au sein de l'Union européenne touchant au secteur de la police et de la justice, notamment ceux relevant du développement de l'acquis de Schengen. Il s'attache à faire entendre sa voix auprès des dif-

férentes autorités compétentes au sein de l'Union européenne et notamment auprès du Parlement européen. Il émet des avis et des propositions concrètes pour garantir la protection des données de manière effective sans entraver la nécessaire coopération policière et judiciaire. Le groupe entend également jouer un rôle dans la coordination d'activités de contrôle coordonnées entre les autorités nationales de protection des données et a entrepris d'élaborer un manuel pour la conduite de tels contrôles.

Autorités de contrôle communes Schengen et Eurodac

Depuis le 12 décembre 2008, la Suisse fait partie de l'espace Schengen. Nous sommes ainsi devenus membres de l'Autorité de contrôle commune Schengen (ACC) et du groupe de coordination Eurodac qui réunit les autorités nationales de protection des données et le contrôleur européen à la protection des données. Ces deux instances de contrôle permettent un large échange d'informations sur l'interprétation des normes de protection des données régissant Schengen et Dublin. L'ACC a notamment pour rôle de coordonner des activités de contrôle régulières et communes pour vérifier le respect des dispositions de protection des données de la convention Schengen et d'adresser aux Etats membres et au Conseil européen les recommandations nécessaires. Nous avons participé à une première inspection concernant les signalements des personnes disparues ou devant être protégées dans le Système d'information de Schengen. Les résultats de cette inspection ne sont pas encore connus. Dans le cadre du groupe de coordination Eurodac, nous avons participé à une enquête relative à l'information des personnes concernées concernant leurs droits. Le rapport final n'a pas encore été élaboré.

Conférence internationale des commissaires à la protection de données

La 30e Conférence internationale des commissaires à la protection des données et à la vie privée a été organisée conjointement par la Commission Nationale Informatique et Libertés (France) et le Commissaire fédéral allemand à la protection des données et à la liberté d'information. Elle s'est tenue à Strasbourg du 15 au 17 octobre 2008 (www.privacyconference2008.org). Sous le thème «Protéger la vie privée dans un monde sans frontières», quelque 570 participants provenant de 60 pays du monde entier et issus des autorités de protection des données, d'organisations internationales, de différents secteurs de l'économie et du monde académique et scientifique ont participé aux travaux et échangé sur les défis actuels pour la protection des données que sont les politiques de sécurité, les réseaux sociaux, les attentes des entreprises et de l'économie en général ou les technologies numériques. Aux yeux des participants, il

est apparu essentiel de renforcer la confiance mutuelle pour développer des solutions, des instruments et des produits qui tiennent compte du droit de la protection des données et en intègrent les exigences. Les commissaires à la protection des données et à la vie privée ont adopté sept résolutions. En particulier dans une résolution sur l'accréditation à la conférence, ils ont accrédité la Croatie et le Burkina Faso; celui-ci est la premier Etat africain ayant adopté une loi de protection des données et mis en place une autorité indépendante de surveillance. Sur proposition conjointe du PFPDT et de l'Autorité espagnole de protection des données, la Conférence a adopté une résolution sur l'urgence de protéger la vie privée dans un monde sans frontières et élaboré une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles. Cette résolution (voir annexe 4.1.7) s'inscrit dans la ligne des résolutions des conférences précédentes et notamment de la déclaration de Montreux adoptée lors de la 27e Conférence (cf. notre 13e rapport d'activités 2005/2006, ch. 9.2.1 et 11.2). Rappelant que le droit à la protection des données et à la vie privée est un droit fondamental des personnes indépendamment de leur nationalité et de leur domicile, les commissaires à la protection des données renouvellent leur appel à l'élaboration d'un instrument juridique contraignant en matière de protection des données et à la vie privée. En ce sens, ils soutiennent notamment les efforts du Conseil de l'Europe en vue de l'adhésion des Etats non membres à la Convention 108 et à son protocole additionnel. La résolution charge également un groupe de travail de rédiger et de soumettre à la prochaine conférence une proposition commune d'établissement de normes internationales sur la vie privée et la protection des données personnelles. La réunion constitutive de ce groupe de travail, auquel nous participons, s'est tenue le 12 janvier 2009 à Barcelone. Elle a permis de fixer la méthode de travail, d'entendre des experts de différents horizons et de faire l'inventaire des problèmes à aborder. La Conférence a en outre adopté une résolution concernant la création d'un comité directeur relatif à la représentation des autorités de protection des données lors des réunions d'organismes internationaux, une résolution sur la création d'un site web de la Conférence, une résolution visant à la mise en place d'une journée ou d'une semaine internationale de la protection de la vie privée et des données personnelles, une résolution sur la vie privée des enfants en ligne (voir annexe 4.1.8) et une résolution sur la protection de la vie privée dans les services de réseaux sociaux (voir annexe 4.1.9).

Association francophone des autorités de protection des données

Nous sommes également actifs au sein de l'Association francophone des autorités de protection des données (AFAPDP), dont nous assurons l'une des 3 vice-présidences. Fondée le 24 septembre 2007 à Montréal, la première année d'existence a permis à l'AFAPDP de se mettre en place et de lancer ses premières activités, notamment par une implication au sein des réseaux institutionnels de l'espace francophone afin de promouvoir le droit à la protection des données personnelles en tant qu'élément essentiel pour la démocratie d'aujourd'hui. L'Association a également commencé d'échanger des informations sur les positions prises par les autorités de protection des données concernant des thèmes d'actualité et a procédé au recensement des textes législatifs des pays de l'espace francophone. L'association participe également aux travaux du Conseil de l'Europe en tant qu'observateur. L'AFAPDP a tenu sa 2e Assemblée générale à Strasbourg en marge de la 30e conférence internationale. Cette Assemblée a été précédée d'une conférence francophone sous forme d'ateliers de sensibilisation et de formation aux bonnes pratiques. Le premier atelier était consacré à l'information des personnes concernées sur leurs droits. Un second atelier a abordé différents aspects techniques touchant à la géolocalisation, à la vidéosurveillance et à la biométrie. Nous avons ainsi eu l'occasion de présenter notre pratique en matière de vidéosurveillance et d'attirer l'attention sur les techniques existantes en matière de protection de la vie privée.

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

Les thèmes abordés par le Groupe de Berlin au cours de l'année écoulée ont été tout particulièrement la problématique des réseaux sociaux sur Internet, la recherche des violations du droit d'auteur sur les bourses d'échange ainsi que les sites de notation sur Internet.

Dans le courant de l'année 2008, le Groupe de travail international sur la protection des données dans le domaine des télécommunications (ou «Groupe de Berlin») s'est réuni en mars à Rome et en octobre à Strasbourg. En raison de la proximité de ces manifestations, le PFPDT a exceptionnellement pu être présent aux sessions du printemps et de l'automne.

Le Groupe de Berlin a adopté à Rome un document sur le thème des réseaux sociaux sur Internet (tels que Facebook, Myspace, etc.). Ces dernières années, les sites de réseautage social ont gagné en popularité, tout particulièrement auprès des jeunes générations. Le document en question («Rome Memorandum»), a pour but d'exposer

les risques que peuvent présenter ces sites du point de vue de la vie privée. Il contient en particulier un certain nombre de recommandations à l'attention de tous les acteurs concernés, à savoir les législateurs, les fournisseurs de sites de réseaux sociaux ainsi que, bien évidemment, leurs utilisateurs. En outre, un symposium international consacré à «la protection de la vie privée à l'ère des réseaux sociaux» a précédé la session d'automne du Groupe de Berlin à Strasbourg.

La thématique du traitement des données personnelles dans le cadre de la lutte contre la violation des droits d'auteur (cf. également notre 15e rapport d'activités 2007/2008, ch. 1.3.1) ainsi que la problématique des sites de notation sur Internet (cf. ch. 1.3.7) ont également été abordés.

Tous les documents publiés par le groupe peuvent être consultés (en anglais et en allemand) sur le site www.iwgpdt.org ou sur le site www.datenschutz-berlin.de, Europa/International – International Working Group on Data Protection in Telecommunications (IWGDPT).

Sur la base du Rome Memorandum, le PFPDT a élaboré à son tour un document sur le thème des réseaux sociaux sur Internet. Ce dernier est disponible sur notre site web www.leprepose.ch, sous la rubrique Thèmes – protection des données – internet – sites de réseautage social.

2 Loi sur la transparence: bilan de l'année 2008

2.1 Demandes d'accès reçues auprès de l'Administration fédérale

Selon les offices fédéraux, le nombre de demandes d'accès et de demandes en médiation a légèrement diminué par rapport à l'année précédente. On peut cependant se demander si toutes les demandes ont effectivement été saisies et communiquées. Le pourcentage des accès (communiqués) qui ont été entièrement ou partiellement accordés est plus ou moins égal à celui de l'année précédente. En ce qui concerne les demandes en médiation, nous avons réussi dans la moitié des cas à obtenir un résultat plus favorable pour le requérant.

C'est déjà la troisième fois que les organes soumis à la loi sur la transparence ont dû nous communiquer combien de demandes d'accès ils ont reçus et comment ils ont tranché. Selon les chiffres qui nous ont été communiqués, les autorités fédérales ont reçu 221 demandes d'accès en 2008. Dans 115 cas, les autorités ont accordé un accès complet et dans 35 cas un accès limité. Dans 71 cas, l'accès aux documents a été refusé. Par rapport à l'année précédente, ces chiffres n'ont pas notablement changé (cf. la statistique au chiffre 3.5).

Ceci permet de conclure et de remarquer ce qui suit:

- Pour 68% des demandes d'accès déposées, un accès complet ou un accès limité a été accordé, dans 32% des cas, l'accès a été refusé.
- Ce qui frappe à nouveau cette année est le nombre élevé de refus et le nombre relativement bas des accès accordés de manière limitée. Même si la part des accès limités a doublé par rapport à l'année passée, on peut constater que les autorités fédérales semblent préférer refuser complètement l'accès plutôt que d'appliquer le principe de la proportionnalité – comme le demande la loi sur la transparence – et d'accorder un accès limité. Nous nous demandons si ceci est dû au fait que l'octroi d'un accès limité demande plus de travail (masquer certaines parties du document, anonymiser, etc.).
- Il y a des unités administratives qui, depuis l'entrée en vigueur de la loi sur la transparence il y a trois ans, ne nous ont pas encore signalé une seule demande d'accès. Il peut y avoir plusieurs raisons à ceci. D'une part, certaines unités administratives avouent ouvertement qu'elles traitent «sans formalité» les demandes émanant du public en accordant sans autre l'accès et ne les incluent

donc pas dans la statistique. Dans cette catégorie, on trouve entre autres les demandes adressées par des journalistes aux services d'information et de communication des différents offices fédéraux. D'autre part, on peut encore toujours admettre qu'un grand nombre de demandes d'accès ne sont pas reconnues comme telles. Cela signifie que la statistique ne contient que les cas considérés comme «importants» par l'office fédéral, c'est-à-dire ceux qui sont difficiles à apprécier ou qui occasionnent une grande charge de travail (par exemple parce qu'ils demandent l'anonymisation de rapports volumineux). Nous en concluons que les chiffres qui nous sont communiqués par les autorités fédérales doivent être interprétés avec prudence. Il est bien probable que le nombre de demandes adressées à l'administration fédérale est plus élevé que ce que la statistique révèle. La même chose vaut probablement pour les demandes qui reçoivent une réponse positive.

- Une autre tendance intéressante qui se dessine est que les offices nous communiquent un nombre plus élevé de demandes d'accès dans les cas où ils ont organisé des séances de formation interne sur la loi sur la transparence et/ou qu'ils disposent d'un système de gestion documentaire qui a été adapté aux exigences de la loi sur la transparence (comme l'OFEV, l'OFCOM et le PFPDT).

- Comme l'année passée, les offices fédéraux ont renoncé en règle générale à demander un émolument pour le traitement des demandes d'accès. Un émolument a été demandé seulement dans 5 des 221 cas qui nous ont été signalés. Le montant total des émoluments encaissés est de CHF 1'280.- (en 2007: CHF 1'730.-).

- Il n'est toujours pas possible d'obtenir des informations fiables sur la charge de travail occasionnée par ces demandes dans les offices et départements. Les autorités fédérales ne sont pas tenues de nous communiquer la charge de travail associée à l'appréciation d'une demande d'accès. Les informations qui nous ont été transmises de plein gré ne sont donc pas vraiment significatives. Selon ces informations, la charge de travail aurait fortement augmenté par rapport à l'année précédente (273 heures en 2007, 509 heures en 2008).

2.2 Demandes d'accès reçues auprès des Services du Parlement

Les Services du Parlement sont également soumis à la loi sur la transparence. Selon les informations qu'ils nous ont communiqué, ils n'ont reçu aucune demande d'accès en 2008.

2.3 Demandes en médiation déposées auprès du PFPDT

En 2008, nous avons reçu en tout 25 demandes en médiation (cf. la statistique au chiffre 3.7). L'année précédente, elles étaient encore au nombre de 36.

En tout, 27 demandes en médiation déposées dans les années 2007 et 2008 ont pu être closes. Dans quatre cas, une solution consensuelle a pu être trouvée avec les parties impliquées. Dans 16 cas, où une solution à l'amiable n'a pas pu être trouvée ou n'était pas envisageable dès le début, nous avons émis des recommandations (dans quelques cas, nous avons pu clore plusieurs demandes en médiation avec une seule recommandation). Dans cinq cas, l'autorité est revenue sur sa décision au cours de la procédure de médiation pour finalement néanmoins accorder l'accès demandé. Dans deux cas, nous avons conclu que la loi sur la transparence n'était pas applicable.

Ces chiffres permettent de conclure et de remarquer ce qui suit:

- Dans 106 cas, les autorités ont complètement refusé l'accès (71) ou ne l'ont accordé que de manière limitée (35). Suite à ces refus complets ou partiels, 25 demandes en médiation ont été déposées chez nous. Cela signifie donc que dans un petit quart des demandes d'accès refusées ou limitées, nous avons par la suite reçu une demande en médiation. L'année passée, ceci était encore le cas pour un tiers des demandes. Ce qui reste inchangé est que ce sont à nouveau les avocats et les journalistes qui ont déposé le plus de demandes en médiation.
- Dans la moitié des procédures de médiation menées à terme (médiations et recommandations), nous avons réussi à trouver une solution plus favorable pour le requérant (à savoir une médiation ou un accès plus étendu que ce qui avait à l'origine été accordé par l'office fédéral).
- La majorité de nos recommandations ont été acceptées par les requérants et les offices fédéraux; dans quatre cas, les requérants ont exigé que l'autorité émette une recommandation. A notre connaissance, aucune de nos recommandations n'a fait l'objet d'un recours auprès du Tribunal administratif fédéral dans l'année écoulée.

Plus d'un office fédéral s'est adressé à nous au cours de la procédure de médiation en nous priant de lui remettre la demande d'accès (qui avait à l'origine été déposée chez lui), parce qu'il n'arrivait plus à mettre la main dessus. C'est avec étonnement que nous avons en outre pris connaissance du fait qu'il existe encore des administrations qui n'ont pas de système de gestion documentaire.

Le nombre de demandes en médiation déposées en 2008 est inférieur à celui de l'année précédente, ce qui nous a permis de traiter une partie des dossiers en retard. Malheureusement, malgré cela certains requérants ont dû attendre encore trop longtemps l'engagement de la procédure de médiation. Il faut toutefois relever que l'exécution rapide d'une procédure de médiation dépend aussi du degré de coopération des autorités fédérales impliquées (par ex. par la remise rapide des documents nécessaires ou la disposition à trouver des solutions au cours d'une séance de médiation). Dans les cas où les requérants demandent l'accès à des documents qui contiennent des données personnelles de tiers, il serait souhaitable que les offices fédéraux entendent effectivement les tiers concernés comme le demande la loi sur la transparence au lieu de refuser d'emblée l'accès en avançant l'argument de la protection de la sphère privée.

2.4 Recommandations

Les recommandations que nous avons émises dans le domaine de la loi sur la transparence au cours de l'exercice écoulé sont résumées brièvement ci-après. Les textes complets sont accessibles dans leur version originale sur notre site web www.leprepose.ch, sous la rubrique Documentation – principe de la transparence – recommandations. Trois recommandations importantes sont publiées dans l'annexe (ch. 4.2.1 – 4.2.3).

Recommandation OFSP / Contrat portant sur un vaccin prépandémique (1er février 2008)

La demande d'une entreprise pharmaceutique à pouvoir accéder à un contrat (portant sur l'achat d'un vaccin prépandémique) conclu avec une autre société a été rejetée par l'Office fédéral de la santé publique en renvoyant à une recommandation précédente émise dans la même cause. Dans une nouvelle recommandation, le Préposé soutient la décision de l'OFSP.

Recommandation OFEV / Listes d'adresses et déclarations de taxe des déponies et des exportateurs de déchets (13 mars 2008)

L'Office fédéral de l'environnement a refusé l'accès aux documents précités. Le Préposé a recommandé à l'office de permettre l'accès à certaines listes d'adresses.

Recommandation Surveillance des fondations / Rapport de révision (11 juin 2008)

L'autorité fédérale de surveillance des fondations a refusé – en se fondant sur le secret professionnel, d'affaires et de fabrication – d'accorder l'accès au rapport de révision, au bilan et au compte de pertes et profits d'une fondation. Dans sa recommandation, le Préposé a soutenu que l'accès a été refusé à juste titre, étant donné que les documents concernés contiennent des informations détaillées sur l'état des revenus et de la fortune de la fondation et que ces informations revêtent une importance primordiale pour les activités de la fondation.

Recommandation DFAE / Dossier de projet DDC (28 juillet 2008)

Le requérant avait déposé plusieurs demandes d'accès concernant des projets en cours du Corps suisse d'aide humanitaire (CSA) et de la Direction du développement et de la coopération (tel que la reconstruction après la catastrophe de tsunami en Asie du Sud). En fin de compte, le Préposé a dû évaluer six demandes en médiation complexes. Dans sa recommandation, il conclut entre autres qu'il était justifié de demander au requérant de préciser sa demande d'accès, que les rapports ne doivent pas être retravaillés et que l'un des rapports devra être anonymisé. La version complète de la recommandation se trouve à l'annexe 4.2.1 (en allemand).

Recommandation DFAE / Rapport sur la politique extérieure en matière d'énergie (29 août 2008)

Le Département fédéral des affaires étrangères a refusé à un requérant l'accès à un rapport concernant la politique extérieure en matière d'énergie en se référant à plusieurs clauses d'exception de la loi sur la transparence. Le Préposé a finalement conclu qu'une publicité de grandes parties du rapport n'enfreignait pas les intérêts de maintien du secret avancés par le DFAE. Il a recommandé d'accorder l'accès au rapport après avoir noirci quelques rares parties du document.

Recommandation OFS / Secret des statistiques (31 octobre 2008)

La requérante avait demandé de pouvoir accéder à la statistique sur le taux de réussite des bacheliers en Suisse romande. L'Office fédéral de la statistique lui a refusé l'accès en se référant au secret des statistiques selon l'art. 14 de la loi sur la statistique fédérale (LSF). Le Préposé a partagé l'avis de l'OFS et émis une recommandation en conséquence. La version complète de la recommandation se trouve à l'annexe 4.2.2.

Recommandation OFAS / Appel d'offres pour des appareils auditifs (28 novembre 2008)

Les requérants souhaitaient consulter deux expertises juridiques relatives à un appel d'offres pour des appareils auditifs par l'Office fédéral des assurances sociales et ont à cet effet déposé une demande d'accès aussi bien auprès de l'OFAS que de la Commission de la concurrence (COMCO). Dans sa recommandation, le Préposé a retenu que la loi sur la transparence n'était pas applicable dans ce cas, étant donné que les documents faisaient partie d'une procédure pendante.

Recommandation Surveillance des fondations / Activité de surveillance (11 décembre 2008)

L'autorité fédérale de surveillance des fondations a refusé à un requérant le droit d'accès à un dossier concernant une fondation, en particulier à des documents concernant le remboursement d'un montant délictueux par l'ancien président du Conseil de fondation. Comme le Préposé l'a constaté dans sa recommandation, l'intérêt public à pouvoir accéder aux documents précités prévaut, dans le cas concret, à l'intérêt des personnes privées concernées (telles que le Conseil de fondation, l'ancien président du conseil de fondation) à protéger leur vie privée. La version complète de la recommandation se trouve à l'annexe 4.2.3 (en allemand).

Recommandation armasuisse / Vente d'un arsenal (15 décembre 2008)

Le requérant avait déposé une demande auprès d'armasuisse – un office du Département fédéral de la défense, de la protection de la population et des sports (DDPS) – pour accéder à divers documents concernant la vente de l'arsenal de Langnau (Emmental). armasuisse a refusé cet accès en argumentant que cette demande d'accès concernait une affaire qui avait été conclue avant l'entrée en vigueur de la LTrans. Cependant, une partie des documents avait été rédigée après l'entrée en vigueur de la LTrans et avait en outre déjà été rendue accessible à un autre requérant. C'est la raison pour laquelle le Préposé a recommandé d'accorder l'accès aux documents, afin de respecter le principe selon lequel tous les requérants doivent avoir les mêmes droits.

Recommandation DFAE / Rapports d'inspection de visas (23 décembre 2008)

Le Département fédéral des affaires étrangères a transmis à un requérant, à sa demande, deux rapports d'inspection de visas de Moscou et de Mumbai, après avoir noirci certaines parties des documents. Le Préposé devait examiner si le caviardage de ces parties de texte était justifié. Il a recommandé de ne caviarder que certains passages.

2.5 Médiations

Les cas suivants ont pu être clos à l'aide d'une médiation:

Médiation OFJ / Norme pénale contre le racisme:

Le requérant avait demandé à l'Office fédéral de la justice de lui accorder un accès à divers documents concernant une audition relative à la norme pénale contre le racisme. Après une discussion constructive au cours de la séance de médiation, le requérant a réussi à concrétiser sa demande et a finalement reçu les documents souhaités.

Médiation RFA / Fichiers d'adresses:

La Régie fédérale des alcools a refusé d'accorder un accès aux listes contenant les adresses des distillateurs et des détenteurs de licences pour le commerce de gros, en invoquant qu'elle ne dispose pas d'une base légale permettant la communication de données personnelles à des tiers. La séance de médiation a permis de se mettre d'accord sur une proposition du préposé: Le requérant a rédigé une lettre d'information que la RFA a expédié aux destinataires souhaités en évitant ainsi de communiquer la liste des adresses au requérant.

Médiation SER / Statistique des bacheliers:

La requérante avait demandé au Secrétariat d'État à l'éducation et à la recherche de lui fournir des informations sur les taux de réussite des bacheliers suisses romands dans les écoles publiques et privées. Les parties impliquées se sont mises d'accord lors de la séance de médiation pour que l'autorité demande aux écoles privées de lui fournir la statistique afin qu'elle puisse, avec l'accord de l'école concernée, la transmettre à la requérante.

Médiation OFS / Poste vacant:

L'Office fédéral de la statistique avait, en invoquant la protection des données, refusé au requérant l'accès à des informations concernant l'affectation d'un poste à l'OFS. Suite à une médiation par téléphone, les documents souhaités ont pu être remis au requérant.

3. Le PFPDT

3.1 Webdatareg: mise en ligne du registre des fichiers

Après avoir mis à jour les déclarations de fichiers effectuées par les offices fédéraux, nous avons adressé une copie des déclarations existantes aux personnes privées et aux entreprises accomplissant des tâches fédérales, afin qu'elles puissent vérifier les données déclarées et les corriger si nécessaire. Nous avons ainsi procédé aux corrections requises et avons en outre étendu le volet internet en introduisant un module permettant la déclaration de fichiers par les nombreux organes fédéraux externes. Outre la déclaration en ligne des fichiers, l'application permet la recherche, la consultation ainsi que l'impression des fichiers déclarés.

Au cours de l'exercice précédent (cf. notre 15e rapport d'activités 2007/2008, ch. 3.1), nous avions déjà formé tous les offices fédéraux concernés au volet intranet de l'application, afin qu'ils puissent déclarer leurs nouveaux fichiers et si nécessaire modifier les déclarations existantes par voie électronique avant l'été 2008.

Conformément à notre planification, nous avons ensuite envoyé au printemps 2008 une copie des déclarations existantes à toutes les personnes privées (entreprises), ainsi qu'à toutes celles accomplissant des tâches fédérales (p. ex. caisses maladie et assurances accident), et leur avons demandé d'en vérifier l'exactitude. Ce publipostage de grande ampleur (plus de 600 envois) a provoqué son lot de retours, questions et problèmes, ainsi qu'un important volume de demandes de correction des données de déclaration. Une fois les nouvelles mutations introduites dans le registre, nous avons encore étendu les fonctionnalités du volet internet de l'application et introduit un module de déclaration de fichiers pour les nombreux organes fédéraux non membres du réseau interne (intranet) de la Confédération (organes fédéraux externes).

Le volet internet de WebDatareg a été mis en ligne en novembre 2008. Celui-ci permet de rechercher, consulter et imprimer les détails de toute déclaration contenue dans le registre et de déclarer les fichiers auprès du PFPDT par le biais d'un formulaire PDF ou XML. Après réception d'une confirmation écrite et signée par le déclarant ainsi authentifié, nous importons ses données de déclaration dans le registre, et assurons au passage la traduction de la dénomination et du but du fichier dans les deux autres langues nationales (cette traduction n'est assurée que pour les déclarations émanant de personnes privées, les organes fédéraux externes étant eux tenus de fournir tous ces éléments).

L'introduction du volet internet du WebDatareg a d'emblée été appréciée par tous les intéressés, notamment en raison de son fonctionnement stable et intuitif. Afin de pouvoir établir et superviser les statistiques de fréquentation, nous avons défini un module d'analyse statistique avec notre prestataire de service d'hébergement, l'Office fédéral de l'informatique et de la télécommunication (OFIT). Ce projet nous a permis d'offrir un outil moderne et efficace pour déclarer et mettre à jour les fichiers, de même que pour rechercher aisément les déclarations contenues dans le registre. Nous sommes convaincus d'avoir ainsi pu réactualiser et revaloriser ce précieux instrument public de transparence qu'est le registre des fichiers.

3.2 3e Journée européenne de la protection des données

La 3e Journée européenne de la protection des données a eu lieu le 28 janvier 2009. Dans ce cadre, différents thèmes ayant trait à la protection des données ont été à nouveau abordés au cours d'émissions de radio organisées dans toute la Suisse. Nous avons en outre participé à différentes manifestations.

La journée de la protection des données, organisée à l'initiative du Conseil de l'Europe, a pour objectif de sensibiliser la population à la protection de la sphère privée. Cette protection a plusieurs facettes. D'une part, le législateur et les préposés à la protection des données travaillent à la mise en place des conditions-cadres pour le traitement des données personnelles. D'autre part, il est de plus en plus important que tout un chacun agisse de manière responsable sur Internet.

A l'occasion de cette journée, Hanspeter Thür, Préposé fédéral à la protection des données, a tenu une conférence à l'Institut Europa de l'Université de Zurich, consacrée aux premiers bilans tirés depuis la révision de la loi fédérale sur la protection des données. Des émissions de radio en Suisse alémanique, en Suisse romande et dans le Tessin ont permis par ailleurs d'aborder divers thèmes d'actualité, comme les sites de réseautage social sur Internet, le cybermobbing et les moteurs de recherche. Citons également parmi les autres thèmes abordés les cartes-clients, le projet de carte-santé et, d'une manière générale, la sensibilisation de la population à la protection des données. Ce dernier thème constitue un objectif permanent de notre travail.

3.3 Publications du PFPDT – Nouvelles parutions

Notre site web est un outil de première importance en matière d'information du public. Durant l'année sous revue, nous avons encore élargi de manière continue notre offre d'informations et publié les résultats de nos travaux. Parmi nos nouvelles publications se trouvent entre autres l'accord établissant une sphère de sécurité entre la Suisse et les Etats-Unis (U.S.-Swiss Safe Harbor Framework), les commentaires concernant les systèmes dits «Pay as you drive», les sites de réseautage social et autres plateformes Internet, ainsi qu'un guide relatif aux systèmes de reconnaissance biométrique.

La révision de la loi sur la protection des données est entrée en vigueur le 1er janvier 2008, en même temps que la révision de l'ordonnance sur la protection des données. Durant la période sous revue, nous avons publié un commentaire à ce sujet sur notre site web www.leprepose.ch sous la rubrique Le PFPDT – bases légales. En outre, les maîtres de fichiers ont désormais la possibilité de faire certifier leurs processus d'exploitation, leurs produits ainsi que leur organisation. Ainsi, au cours de l'année écoulée, nous avons accompli le mandat qui nous était attribué par la loi et avons établi des directives, publié des commentaires ainsi que d'autres informations concernant les certifications en matière de protection des données. Ces documents se trouvent sous la rubrique Thèmes – protection des données.

De plus, la révision de la loi a entraîné des modifications au niveau de la transmission de données à l'étranger. Toujours sur notre site, nous avons mis en ligne à la rubrique Thèmes – protection des données – transmission à l'étranger une version brève et une version plus détaillée de nos explications à ce sujet. On trouvera également au même endroit l'accord établissant une sphère de sécurité entre la Suisse et les Etats-Unis (U.S.-Swiss Safe Harbor Framework), négocié en collaboration avec le SECO.

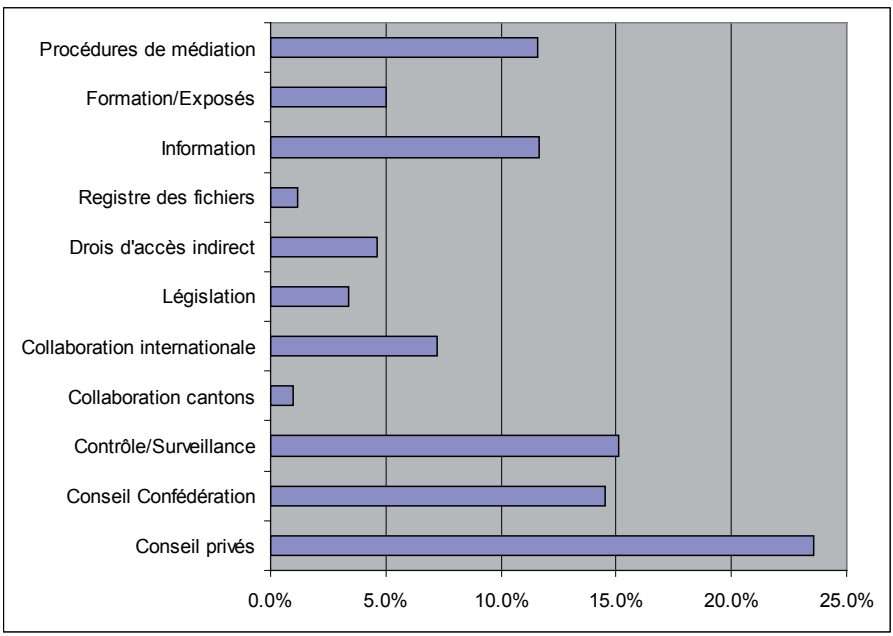
Les nouvelles technologies placent aujourd'hui la protection des données face à de grands défis. Il nous est donc paru nécessaire de fournir des explications sur les développements les plus récents, notamment au sujet des systèmes dits «Pay as you drive» dans le domaine des assurances des véhicules à moteur. Si le comportement du conducteur assuré est enregistré sur une boîte noire, les principes de la protection des données doivent être respectés. Il en va de même de l'enregistrement du comportement des spectateurs dans le domaine de la télévision numérique. En effet, on peut établir des profils de la personnalité des personnes concernées; ceux-ci doivent être traités avec un soin particulier. Le commerce par téléphone portable est également un sujet très actuel. De plus en plus de personnes profitent des systèmes de

paiement permettant de régler leurs factures à l'aide d'un téléphone portable. Nous avons exposé les risques inhérents à ces systèmes et les mesures à observer dans un texte intitulé «Explications concernant le paiement par téléphone portable». La téléphonie par Internet, ou Voice over IP (VoIP), fait aussi de plus en plus d'adeptes. Les communications VoIP utilisant les canaux Internet usuels, le risque est grand qu'une conversation téléphonique soit illicitement interceptée. Les utilisateurs doivent donc prendre les mesures de sécurité qui s'imposent. Internet est également un thème d'actualité à d'autres égards. Mentionnons tout d'abord les sites de réseautage social comme Facebook ou MySpace qui connaissent un essor considérable. Ils impliquent des risques plus ou moins bien connus pour la personnalité des utilisateurs, mais aussi des personnes qui ne participent pas à de tels sites. Par ailleurs, les sites d'évaluation se sont multipliés au cours de l'année écoulée, au niveau tant international que régional. Ces sites permettent de diffuser toutes sortes d'évaluations, de l'attitude de son voisin aux prestations de son médecin en passant par les cours donnés à l'université. Nous y avons aussi consacré nos réflexions durant l'année sous revue et les avons présentées dans des commentaires spécifiquement consacrés à ce sujet ainsi que dans les deux éditions de notre newsletter datum. Enfin, le dernier thème qui nous a préoccupés dans ce domaine est la protection des jeunes face aux appareils automatiques. En Allemagne, des exploitants d'appareils automatiques et des établissements de crédit ont mis au point des systèmes permettant de procéder à un contrôle de l'âge aux automates. Nous avons examiné ces systèmes sous l'angle de la protection des données. Toutes ces explications peuvent être consultées sur notre site sous Thèmes – protection des données, aux chapitres correspondants.

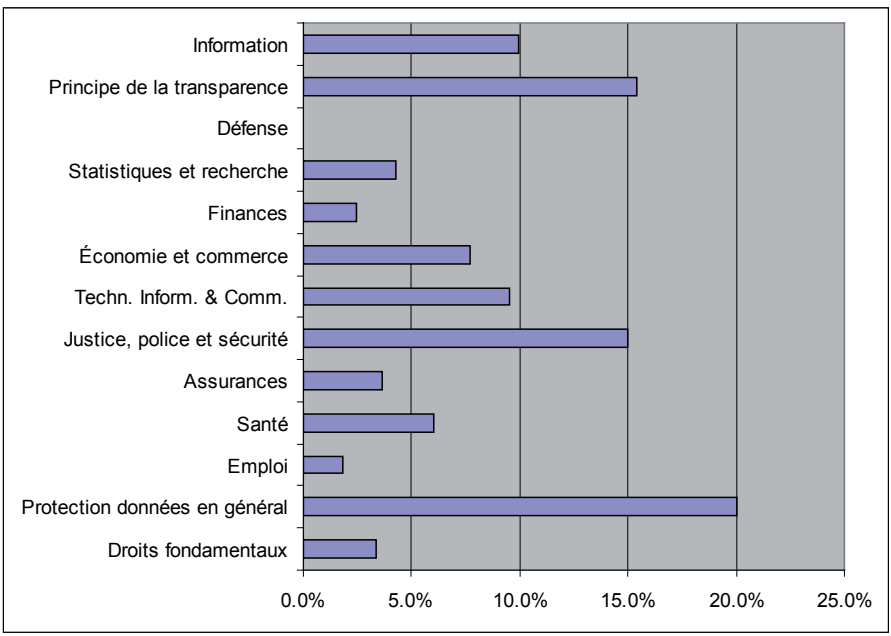
La société actuelle a de plus en plus tendance à installer des systèmes d'accès et de reconnaissance biométriques. Nous avons publié un guide spécialement conçu pour les développeurs et exploitants de ces systèmes. Ce guide se trouve sur notre site sous Documentation – protection des données – brochures.

3.4 Statistique des activités du Préposé fédéral à la protection des données. (Période du 1er avril 2008 au 31 mars 2009)

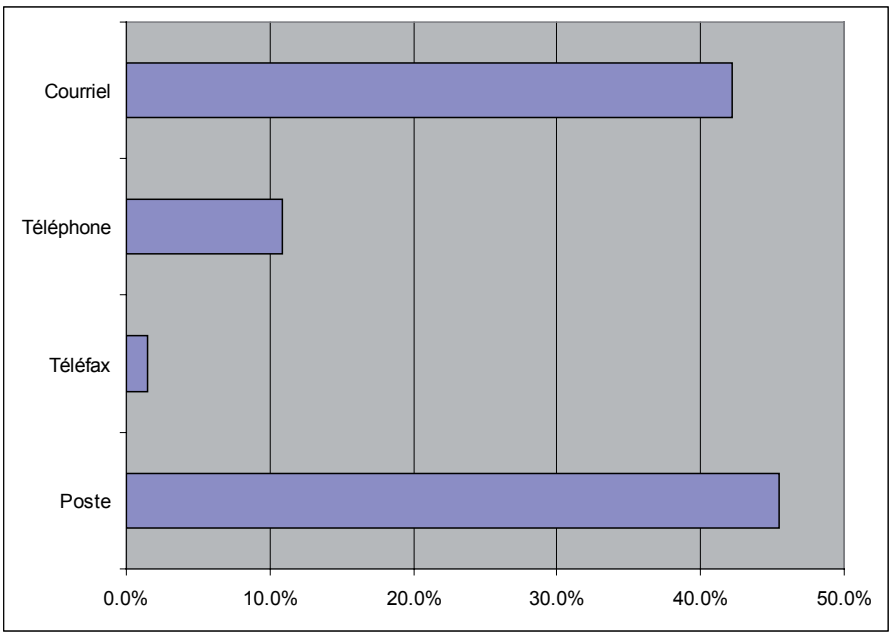
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.5 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2008 au 31 décembre 2008)

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
ChF	31	22	3	6
DFAE	20	11	7	2
DFI	29	9	11	9
DFJP	34	19	12	3
DDPS	18	10	3	5
DFF	18	8	7	3
DFE	11	7	2	2
DETEC	60	29	26	5
TOTAL 2008 (en %)	**221** (100%)	**115** (52%)	**71** (32%)	**35** (16%)

TOTAL 2007 (en %)	**249** (100%)	**147** (59%)	**82** (33%)	**20** (8%)

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
ChF	8	6	0	2
PFPDT	23	16	3	4
TOTAL	**31**	**22**	**3**	**6**

Département fédéral des affaires étrangères DFAE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
TOTAL	20	11	7	2
DFAE	**20**	**11**	**7**	**2**

Département fédéral de l'intérieur DFI

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFI	5	4	1	0
BFEG	0	0	0	0
OFC	1	0	1	0
AFS	0	0	0	0
MétéoSuisse	0	0	0	0
OFSP	8	3	1	4
OFS	0	0	0	0
OFAS	7	0	4	3
SER	2	1	0	1
Conseil des EPF	0	0	0	0
SWISSMEDIC	5	1	3	1
FNS	0	0	0	0
SUVA	1	0	1	0
TOTAL	**29**	**9**	**11**	**9**

Département fédéral de justice et police DFJP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFJP	5	0	4	1
OFJ	4	4	0	0
FEDPOL	5	3	0	2
METAS	0	0	0	0
ODM	15	12	3	0
MPC	3	0	3	0
ISDC	0	0	0	0
IPI	2	0	2	0
CFMJ	0	0	0	0
CAF	0	0	0	0
ASR	0	0	0	0
TOTAL	**34**	**19**	**12**	**3**

Département fédéral de la défense, de la protection de la population et des sports DDPS

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DDPS / BIG	11	8	0	3
Défense/armée	3	0	2	1
armasuisse	1	0	1	0
OFPP	1	0	0	1
OFSPO	2	2	0	0
TOTAL	**18**	**10**	**3**	**5**

Département fédéral des finances DFF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFF	2	0	2	0
AFF	0	0	0	0
OFPER	0	0	0	0
AFC	3	2	1	0
AFD	1	0	0	1
RFA	3	1	0	2
OFCL	0	0	0	0
OFIT	0	0	0	0
OFAP	3	0	3	0
CDF	6	5	1	0
PUBLICA	0	0	0	0
CC	0	0	0	0
TOTAL	**18**	**8**	**7**	**3**

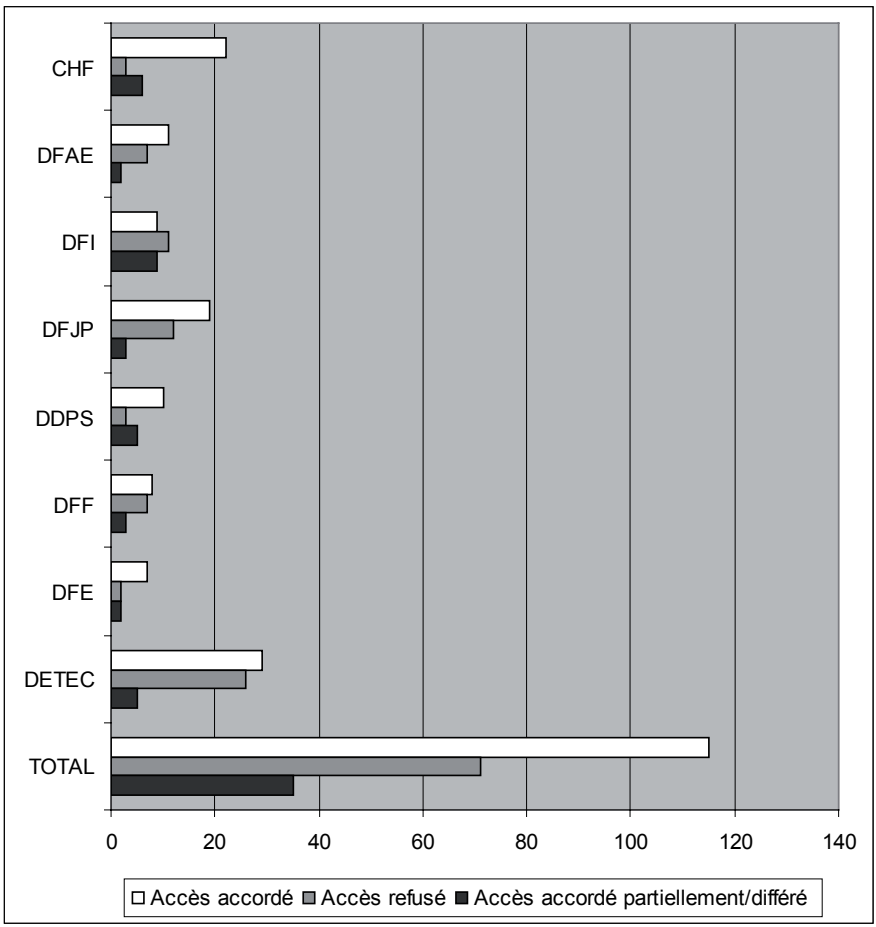
Département fédéral de l'économie DFE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DFE	4	4	0	0
SECO	2	2	0	0
OFFT	1	0	0	1
OFAG	2	1	1	0
OVF	1	0	0	1
OFAE	0	0	0	0
OFL	0	0	0	0
SPr	0	0	0	0
COMCO	1	0	1	0
ZIVI	0	0	0	0
BFC	0	0	0	0
TOTAL	**11**	**7**	**2**	**2**

Département fédéral de l'environnement, des transports, de l'énergie et de la communication DETEC

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SG DETEC	2	0	1	1
OFT	4	1	2	1
OFAC	20	11	9	0
OFEN	2	0	2	0
OFROU	1	0	1	0
OFCOM	8	5	3	0
OFEV	15	6	6	3
ARE	0	0	0	0
COMCOM	0	0	0	0
IFSN	5	3	2	0
PostReg	1	1	0	0
AIEP	2	2	0	0
TOTAL	**60**	**29**	**26**	**5**

Traitement des demandes d'accès



3.6 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2008 au 31 décembre 2008)

Services du Parlement SP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé
SP	0	0	0	0
TOTAL	**0**	**0**	**0**	**0**

3.7 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2008 au 31 décembre 2008)

Catégorie de requérants	2008
Avocats	7
Médias/journalistes DFAE	6
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	6
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	3
Universités	2
Entreprises	1
Total	**25**

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

Préposé fédéral à la protection des données et à la transparence:	
	Thür Hanspeter, Fürsprecher
Suppléant:	Walter Jean-Philippe, Dr. iur.
Secrétariat:	
Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité 1:	9 personnes
Unité 2:	12 personnes
Unité 3:	2 personnes
Chancellerie:	3 personnes

4 Annexes

4.1 Protection des données

4.1.1 Observations concernant les sites de réseautage social

Aujourd'hui, les jeunes, tout particulièrement, passent une bonne partie de leur vie sociale sur la Toile, tendance que vient renforcer l'évolution fulgurante des nouvelles technologies de la communication. Le fait que de plus en plus d'informations d'ordre privé soient mises sur Internet crée des problèmes sous l'angle de la protection des données. Dans ce document, le PFPDT expose les dangers que les sites de réseautage social recèlent pour la sphère privée et donne des recommandations aux personnes concernées afin qu'elles protègent mieux leurs données personnelles.

De plus en plus fréquemment, les utilisateurs d'Internet ne sont plus de simples consommateurs qui cherchent et téléchargent des informations sur des sites Web statiques mis à disposition par des fournisseurs, mais utilisent Internet de façon plus interactive que jamais et participent intensément à l'élaboration de sites Web dynamiques. Cette évolution porte le nom de «Web 2.0». Cette utilisation différente d'Internet a été favorisée à la fois par la diffusion croissante de la technologie à large bande, qui a considérablement accéléré les processus de mise en ligne et de téléchargement, et par le développement de logiciels de réseautage social, qui permettent à un nombre croissant d'utilisateurs de placer bonne quantité de leurs propres contenus sur Internet et de nouer contact.

Différents sites de réseautage social (SRS) ont vu le jour. Il s'agit de vastes portails sur lesquels des utilisateurs enregistrés se rencontrent, tissent des liens d'amitié et échangent des nouvelles, des photos et des films. A cet effet, il suffit de remplir un profil personnel comprenant des informations plus ou moins détaillées sur sa personne, ses préférences et ses convictions. Les SRS les plus connus (facebook, MySpace, StudiVZ etc.) comptent de plus en plus de membres.

Face à l'émergence de ce phénomène, la protection des données doit relever de nouveaux défis. La législation en la matière visait initialement à protéger les données personnelles contre tout traitement illicite ou disproportionné par l'Etat, puis, par l'économie. Deux aspects fondamentalement nouveaux doivent être relevés à cet égard:

1. Ce sont les utilisateurs eux-mêmes qui enregistrent les informations personnelles en question dans les profils Internet et qui donnent donc ainsi leur propre consentement.

2. Les particuliers sont ainsi en mesure d'accéder aisément aux données personnelles d'autres particuliers, ce qui peut engendrer des risques.

Les SRS offrent de nombreux avantages à la société, tels que la possibilité de pratiquer le réseautage, de nouer des contacts au-delà des frontières ou de publier des contenus personnels. Le but de ces observations ne consiste donc pas à condamner ces sites, mais bien plus à sensibiliser les autorités, les fournisseurs et les utilisateurs afin que, dans le cadre du réseautage social, les données personnelles soient traitées de façon correcte et dans le respect de la protection des données.

Dangers potentiels

Sous nos latitudes, Internet est devenu incontournable dans le monde professionnel et dans la vie privée. Il recèle toutefois des dangers bien connus, qui planent aussi sur les SRS. Des personnes mal intentionnées peuvent par exemple tirer profit de la redéfinition des notions de «confiance» et de «confidentialité» qui caractérise ces sites. Lorsque l'amitié revêt des aspects avant tout quantitatifs, il est aisé, sous couvert de mensonges, voire d'une fausse identité, de devenir «l'ami» de quelqu'un et d'obtenir ainsi des informations que «l'interlocuteur» n'aurait peut-être pas révélées lors d'un face à face. L'affirmation des exploitants de tels sites, selon laquelle on ne fait que transférer la communication quotidienne entre amis sur le Net, implique une intimité qui n'existe en fait pas dans un média mondialisé, d'autant moins lorsque l'accès au réseau est relativement facile.

Quiconque utilise les SRS sans mesures de précaution court les risques suivants:

1. La mémoire d'Internet est infaillible: les profils d'utilisateurs peuvent être téléchargés et enregistrés par d'autres utilisateurs, ce qui voue pratiquement à l'échec toute tentative d'effacer le profil d'origine, puisque les données sont ainsi conservées. Des fichiers privés voient le jour un peu partout, ce qui accroît le risque que les données soient utilisées dans un but autre que celui qui était initialement prévu. Publiées hors du contexte des SRS, ces données peuvent en effet nuire considérablement à la personne concernée. De tels

fichiers privés permettent aussi de suivre des modifications apportées par le titulaire d'un profil et de classer les données par catégories selon des critères précis, p. ex. au moyen de la fonction RECHERCHE.

2. Les fournisseurs de SRS ont accès non seulement aux données personnelles, mais aussi aux métadonnées (durée de la connexion, origine géographique plus ou moins précise de l'adresse IP, durée de la consultation du site et pages Web visitées, etc.). Beaucoup de fournisseurs de SRS ne précisent pas ce qu'ils font des données. Une chose est néanmoins certaine: ajoutées aux métadonnées, les données personnelles sont susceptibles de livrer des profils de la personnalité détaillés, dont la vente peut engendrer de juteux bénéfices.

3. Les photos de personnes reconnaissables assorties de leur nom permettent de les identifier clairement. A l'aide d'un logiciel de reconnaissance faciale approprié, on peut passer au crible des SRS et d'autres plates-formes pour y rechercher des personnes précises. Ensuite, on a tôt fait d'identifier ces personnes sur des sites où elles préfèreraient rester anonymes, notamment sur un site de rencontres, ou - grâce à la photo publiée sur le SRS - de faire le lien entre ces personnes et leur CV placé sur le site d'une entreprise.

4. La recherche d'images par le contenu («content based image retrieval»: CBIR) présente des risques similaires: la reconnaissance automatique d'éléments à l'arrière-plan d'une image, p. ex. un tableau ou un bâtiment spécifiques, peut permettre de situer l'endroit où la photo a été prise et de déterminer l'adresse de la personne, ce qui peut faciliter le harcèlement ou d'autres actes criminels.

5. Certains SRS permettent - sans l'autorisation des personnes concernées - de créer des liens vers des profils ou des adresses électroniques de tiers, même lorsque ces derniers ne sont pas membres du réseau. Cela peut mettre en danger la sphère privée de tout un chacun.

6. Il est pour ainsi dire impossible d'effacer définitivement un compte d'utilisateurs (cf. point 1). Les profils sont parfois uniquement désactivés au lieu d'être effacés. En outre, les utilisateurs actifs laissent, sur d'autres pages du réseau, de nombreuses informations supplémentaires qu'il est presque impossible d'effacer dans leur intégralité. Les utilisateurs perdent ainsi le contrôle de leurs données.

7. Il convient aussi de citer les attaques de type «Cross Site Scripting» et les maliciels. En exploitant des failles dans la sécurité informatique, des personnes mal intentionnées injectent p. ex. des codes malicieux dans le but de mettre la main sur des données sensibles de l'utilisateur ou d'infliger des dommages à son ordinateur ou à son profil.

8. Les utilisateurs de différents SRS peuvent simplifier la gestion de leurs boîtes de messagerie en les insérant dans une application Web qui permet de voir d'un coup d'œil tous les messages reçus. Cette application ne nécessite toutefois qu'un seul nom d'utilisateur et un seul mot de passe, ce qui compromet sérieusement la sécurité.

9. On entre comme dans un moulin sur la plupart des SRS: quelques indications personnelles, qui ne sont pas vérifiées et peuvent donc être inventées de toutes pièces, suffisent. Une fois qu'on est sur le site, il est parfois très simple de nouer des contacts et d'être intégré aux cercles d'amis d'autres personnes. Par conséquent, ces communautés risquent d'être infiltrées dans des buts peu louables:

   a. Hameçonnage («phishing»): des malfaiteurs obtiennent ainsi de nombreuses informations qui leur permettent de lancer des attaques de hameçonnage ciblées dans le but de récupérer notamment des données d'accès à des comptes importants ou à des informations bancaires précieuses.

   b. Pollupostage («spamming»): les polluposteurs, à l'instar des utilisateurs inoffensifs, peuvent créer des profils. Le fameux problème du pollupostage risque ainsi d'affecter également les systèmes de communication internes des SRS.

   c. Vol d'identité: le vol d'identité devient simple comme bonjour: il suffit de se créer un profil avec le nom d'une personne connue pour profiter de sa notoriété ou nuire à sa réputation en adoptant un comportement malveillant. Le voleur peut aussi créer un profil au nom d'une personne issue de son école ou de son voisinage à qui il veut faire du tort. Il peut ainsi la ridiculiser ou envoyer des méchancetés en son nom.

10. Le cyber-harcèlement («cyberstalking») est un phénomène récent: les possibilités de contact électroniques offertes par les SRS peuvent être utilisées par des personnes mal intentionnées pour harceler quelqu'un. En outre, vu la quantité de données personnelles dévoilées par les utilisateurs, le harceleur a toutes les chances de trouver l'adresse de sa victime, de connaître son emploi du temps et de la persécuter physiquement.

11. La cyberintimidation («cyberbullying») est la version Internet d'un phénomène connu de longue date dans la vie réelle. L'intimidateur peut se cacher derrière un profil falsifié, rester dans l'anonymat et exploiter les possibilités offertes par les SRS pour harceler une personne ou l'humilier. Il peut le faire au vu et au su des autres membres de la communauté, ce qui porte encore plus préjudice à la victime.

Les services de réseautage social sont le plus souvent gratuits, mais ce ne sont pas des institutions d'intérêt public. Il y a «marchandage»: ils offrent des prestations aux utilisateurs en échange des données personnelles de ces derniers. Derrière ces portails se cache un pouvoir commercial redoutable incarné par de puissantes multinationales qui doivent générer des profits croissants sous la pression des investisseurs et des actionnaires. Les SRS n'ont que des données personnelles à offrir; la valeur boursière de certains de ces sites en dit long sur l'intérêt que présentent ces données.

Le réseautage social sur la Toile est un phénomène relativement récent, que l'on étudie petit à petit. Il est probable que de nouveaux dangers et de nouvelles failles apparaissent à l'avenir.

Recommandations aux autorités[1]:

Dans le but d'améliorer la protection des données, nous formulons les recommandations suivantes:

- Sensibiliser les utilisateurs des SRS aux dangers. Les fabricants de logiciels doivent être encouragés à tenir compte de la sécurité des données personnelles.

[1] Les présentes recommandations reposent pour l'essentiel sur le Rome Memorandum du International Working Group on Data Protection in Telecommunications (cf. bibliographie à la fin du texte)

- Créer un droit, pour l'utilisateur, d'utiliser des SRS sous un pseudonyme.
- Accroître la transparence: il convient de passer au crible, sous l'angle de la législation sur la protection des données, les méthodes de traitement de données pratiquées par les fournisseurs de SRS et, le cas échéant, d'inciter ceux-ci à les améliorer. Les utilisateurs devraient être informés en toute transparence du but visé par le traitement des données, d'une éventuelle transmission de ces dernières ou de leur droit à accéder aux données et à les rectifier.
- Faire attention aux interdictions: au lieu d'interdire l'utilisation de SRS, les écoles devraient (en partie) les autoriser afin d'éviter que le réseautage social échappe à tout contrôle. Ce serait aussi l'occasion d'informer les enfants, les enseignants et les parents.
- Prévoir l'obligation, pour les fournisseurs de SRS, de communiquer des failles dans la sécurité. Les utilisateurs seraient ainsi informés, et on pourrait voir en même temps le niveau de sécurité qu'offre un SRS.
- Enseigner la protection des données: étant donné l'engouement pour les moyens de communication modernes chez les enfants et les adolescents, la protection des données doit absolument être enseignée dans les écoles.

Recommandations aux fournisseurs:

- Prévoir une meilleure authentification des utilisateurs, p. ex. par confirmation postale.
- Améliorer les possibilités, pour les utilisateurs, de dénoncer sur le site, p. ex. à l'aide d'un bouton spécial, les abus et les violations des règles établies.
- Choisir des paramètres standards appropriés: on sait par expérience que peu d'utilisateurs modifient d'eux-mêmes les paramètres initiaux; dans l'optique de la protection des données, il est par conséquent essentiel que les paramètres standards soient conformes à la protection des données.
- Créer la possibilité, pour les utilisateurs, de surfer sous un pseudonyme et les encourager à le faire.
- Donner des informations claires concernant le traitement des données et une transmission éventuelle à des tiers; en outre, s'ils veulent inspirer confiance, les fournisseurs doivent tenir leurs promesses.

- Permettre aux utilisateurs de s'évaluer les uns les autres dans le respect de conditions strictes. Puisqu'ils sont amateurs de SRS, ils peuvent ainsi communiquer à d'autres utilisateurs leurs expériences avec leur «interlocuteur», ces renseignements pouvant être précieux pour des tiers. Les utilisateurs sont ainsi encouragés à adopter un comportement irréprochable afin de se forger une bonne réputation sur la Toile.
- Installer des outils de filtrage automatiques, qui réagissent à certains critères.
- Permettre à l'utilisateur de mieux contrôler ses données:

    - Prévoir la possibilité d'effacer complètement des données.
    - Interdire l'insertion de balises (p. ex. titres des images) contenant des données personnelles sans l'autorisation de la personne concernée.
    - Permettre à l'utilisateur de choisir quelles données apparaîtront dans la fonction RECHERCHE du SRS.
    - Veiller à ce que l'utilisateur puisse contrôler en tout temps ce qu'il advient des données contenues dans son profil et de celles qui permettent de retracer ses mouvements sur la Toile.

Recommandations aux utilisateurs:

- Prenez des précautions avant de publier sur un SRS vos coordonnées (nom, adresse, numéro de téléphone) ainsi que toute autre donnée ou information personnelle (p.ex. convictions politiques). Utilisez des pseudonymes.
- Avant de publier des données, demandez-vous toujours si, lors d'un entretien d'embauche, vous souhaiteriez être confronté aux données/images en question, et cela, même dans dix ans. A l'heure actuelle, il semble que les deux tiers des chefs des ressources humaines passent au crible les SRS et Google pour obtenir des informations sur les candidats.
- Respectez la sphère privée de tierces personnes, ne publiez pas leurs données personnelles et ne mettez pas leur nom sur des photos.
- Informez-vous au sujet des fournisseurs du portail et de la manière dont ils assurent la protection de la sphère privée des utilisateurs. Le service en question dispose-t-il d'un label de qualité en matière de protection des données ou de sécurité? Soyez critique à l'égard du comportement du fournisseur.

- Choisissez dans la configuration de votre profil les options permettant de préserver votre vie privée. Limitez l'accès à vos informations et photos à un cercle de personnes déterminé. Ne mettez jamais de contenus délicats sur Internet.
- N'employez pas le même nom d'utilisateur ni le même mot de passe pour tous les services.
- Surveillez les activités de vos enfants sur Internet.

Divers organes européens se sont déjà penchés sur la question. Pour de plus amples informations, vous pouvez consulter les adresses suivantes:

http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_reputation_based_system.pdf

4.1.2 Explications concernant les plateformes d'évaluation en ligne (novembre 2008)

1 Introduction

Le réseau informatique mondial d'Internet représente la plus grande communauté au monde, donnant librement accès, en tout temps et en tout lieu, aux informations les plus diverses et réalisant de ce fait l'utopie d'une bibliothèque universelle du savoir. Un simple clic permet à tout un chacun de découvrir les dernières percées scientifiques, de lire un journal avant même qu'il ne sorte de presse, de savoir à quelle heure ouvre la boulangerie du coin ou de retrouver la trace d'un camarade d'école.

L'avènement des réseaux sociaux, dans le sillage de l'évolution participative d'Internet, a vu l'émergence d'une nuée d'applications, telles que les plateformes d'évaluation, qui permettent aux internautes d'échanger des informations. Ce n'est alors plus l'administrateur du site qui publie l'information: son rôle se réduit à mettre l'outil, à savoir son site, à la disposition des internautes, qui sont invités à y ajouter leur propre contenu, accessible à tous ou à un groupe déterminé de personnes. Le plus souvent, l'administrateur du site n'effectue aucun contrôle rédactionnel.

123 Jamais jusqu'ici le contenu d'un site n'avait été aussi indépendant de son support. Les conséquences en sont considérables, notamment du point de vue de la garantie et l'imposition des droits de la personnalité. De nombreux administrateurs ne sont en effet plus responsables du contenu de leur site et ne sont pas en mesure de le contrôler, sans compter l'augmentation continue du nombre de pages sur la Toile. Ces facteurs constituent autant de défis importants pour la protection de la personnalité en général et pour la protection des données en particulier.

1.1 Développements et défis des plateformes d'évaluation

L'intérêt à disposer d'informations et d'évaluations sur certains types de prestations est né bien avant l'émergence d'Internet. Les tests et les notations sont ainsi pratiqués depuis de nombreuses années (associations de défense des consommateurs, guides de voyage ou de restauration, etc.).

Les fournisseurs traditionnels d'évaluations appliquent le plus souvent une approche qualitative: ils chargent des experts d'examiner une prestation ou un produit selon certains critères, avant de réunir les résultats de l'étude dans un rapport; ils publient ensuite ce rapport sous leur nom propre, à titre d'expertise. Les fournisseurs portent donc la responsabilité du contenu de la publication, notamment sous l'angle qualitatif.

Il existe cependant une autre méthode d'évaluation, fondée cette fois sur une approche quantitative: un nombre suffisamment élevé de réponses permet en effet d'obtenir des résultats significatifs du point de vue statistique et d'en tirer des conclusions sur la qualité d'un produit ou d'une prestation. Étant donné qu'un grand nombre d'utilisateurs ou de consommateurs doivent être interrogés, l'approche quantitative se révèle toutefois trop astreignante et trop coûteuse dans la plupart des cas pour les fournisseurs d'évaluations traditionnelles.

Les études quantitatives se sont développées avec Internet, qui permet de récolter des informations par voie électronique à moindre coût. La qualité de telles études repose en grande partie sur les modèles mathématiques utilisés pour juger de la fiabilité des résultats. La qualité d'une évaluation quantitative dépend donc de la manière dont les données sont traitées, tandis que la qualité d'une évaluation qualitative dépend des compétences de l'expert mandaté.

L'apparition des sites d'évaluation sur Internet a vu l'émergence d'une forme hybride des deux types d'évaluation précités. Si ces sites fixent un canevas destiné à récolter des informations sous une forme structurée de la part d'un grand nombre d'utilisateurs, ils donnent aussi la possibilité aux utilisateurs de faire des commentaires d'ordre qualitatif dans des champs *ad hoc*.

Toutefois, le dépouillement et la présentation de ce type hybride d'évaluations suivent souvent l'approche qualitative, le nombre de réponses obtenues ne permettant pas de tirer des résultats significatifs du point de vue statistique. Sauf exception, les personnes qui procèdent à l'évaluation ne sont cependant pas des experts spécialement formés qui appliquent des méthodes scientifiques, mais des utilisateurs moyens d'Internet qui donnent leur avis.

La fiabilité et le caractère représentatif des informations obtenues par le biais de ce type d'évaluations sont donc sujets à caution.

1.2 Plateformes d'évaluation sur Internet

Internet héberge plusieurs types de plateformes d'évaluation. Souvent, elles sont intégrées à d'autres plateformes (p. ex. boutiques en ligne ou sites de ventes aux enchères en ligne), mais il existe aussi des plateformes d'évaluation autonomes, entièrement consacrées à l'évaluation de tel ou tel groupe-cible ou de telle ou telle personne (p. ex. évaluation de médecins ou de cours).

1.2.1 Plateformes intégrées

Les plateformes d'évaluation intégrées sont généralement liées à l'achat d'un produit (p. ex. sur une place de marché électronique ou sur un site de vente aux enchères) ou d'un service (p. ex. utilisation d'un site d'échange de vidéos). La transaction terminée, le vendeur ou le client sont priés de procéder à une évaluation, le plus souvent en attribuant une note et en faisant un commentaire.

L'objectif de telles plateformes étant d'évaluer immédiatement une action spécifique, l'évaluation a lieu directement après l'acte de consommation et le consommateur peut être mis en relation directement au produit ou au service Les plateformes intégrées ne posent donc généralement pas de problèmes, pour autant qu'elles ne contiennent aucun jugement de valeur diffamatoire, inutilement dénigrant ou offensant. Notons par ailleurs que, le plus souvent, la conception de ces plateformes ne permet de procéder à une évaluation qu'après une transaction (commande d'une vidéo, achat d'un produit ou d'un service). En outre, dans de nombreux cas (p. ex. lorsque la transaction est payante), l'utilisateur doit s'être enregistré.

D'un point de vue économique, les plateformes d'évaluation intégrées ont principalement pour but d'asseoir la réputation des vendeurs de produits ou de services. Comme aucun contact personnel n'est possible sur Internet et qu'il est difficile de personnaliser les rapports dans un monde virtuel, ces plateformes sont utilisées pour augmenter la confiance des consommateurs dans les vendeurs. Les utilisateurs se sentent dès lors davantage en sécurité.

1.2.2 Plateformes autonomes

Contrairement aux plateformes intégrées, les plateformes d'évaluation autonomes ont principalement pour but d'informer le public sur la qualité de telle ou telle prestation. Les domaines d'application sont variés, allant des recettes de cuisine aux voyages à forfait en passant par l'évaluation d'entreprises ou de particuliers appartenant à une certaine catégorie de personnes (p. ex. les médecins, les enseignants ou les professeurs).

Les différences de fonctionnement de ces sites sont minimes: dans la plupart des cas, un élément s'affiche à l'écran (professeur, cours, médecin ou simple image) et l'utilisateur est invité à l'évaluer au moyen d'un formulaire prédéfini, en attribuant une note allant de 1 à 6 (échelle de Likert), et d'un champ de commentaires.

Selon le site, les utilisateurs peuvent publier eux-mêmes l'élément à évaluer ou celui-ci est imposé par l'administrateur. Le tableau ci-dessous présente les différentes manières de publier l'élément à évaluer.

Publication de l'élément à évaluer (par ex. professeur, cours)		
Par la personne concernée	Par l'administrateur du site	Par tout utilisateur du site

Tableau 1

Pour procéder à une évaluation, l'utilisateur doit le plus souvent s'être enregistré sur le site Internet en question. Certains sites autorisent cependant les évaluations anonymes. Le tableau ci-dessous présente les différents degrés de restrictions à la liberté d'évaluer.

Liberté d'évaluer		
Tout utilisateur, même anonyme	Uniquement après enregistrement	Uniquement sur autorisation

Tableau 2

Les différentes catégories exposées dans les deux tableaux ci-dessus permettent de classer et de juger les différents sites d'évaluation sous l'angle de la protection des données. Les précautions que les administrateurs doivent prendre pour récolter des évaluations et en publier les résultats ne seront donc pas les mêmes selon la manière dont le site a été conçu.

2 Exemples

Nous décrivons ci-dessous trois types de plateformes d'évaluation autonomes rencontrés sur Internet: les évaluations d'images et de vidéos (2.1), les évaluations de médecins (2.2) et les évaluations de cours dans les hautes écoles (2.3).

2.1 Évaluation d'images et de vidéos

Certains sites permettent à des personnes de publier des images ou des vidéos (d'elles-mêmes ou de tiers) et de les faire évaluer par d'autres utilisateurs. Les visiteurs du site Internet voient ainsi s'afficher une image ou une vidéo, prise au hasard dans la banque, et un message leur demandant de lui attribuer une note allant de 1 à 10. Une fois qu'ils se sont exécutés, les résultats provisoires du sondage leur sont communiqués.

Ces sites sont conçus pour que l'élément à évaluer (p. ex. une photo) soit publié par la personne concernée. Les utilisateurs peuvent rester anonymes, mais ils doivent avoir vu l'élément en question pour l'évaluer.

Du point de vue de la protection des données, ce type de site ne pose pas de problèmes, pour autant qu'il garantisse que seule la personne concernée puisse publier des images la représentant. L'utilisateur ayant uniquement la possibilité d'évaluer l'image qui lui est montrée, l'anonymat ne pose pas davantage de problèmes.

2.2 Évaluation de médecins

Les sites d'évaluation de médecins permettent de chercher un médecin (à partir de son nom, de la ville ou du canton où il exerce ou de sa spécialité) et de l'évaluer selon différents critères (accueil et équipe, administration et médecin lui-même) sur une échelle allant de 1 à 6 (ou «sans avis»).

C'est l'administrateur du site qui publie le nom des médecins évalués. Les utilisateurs pouvant évaluer le médecin anonymement, rien ne les empêche d'évaluer un médecin qui ne les a jamais traités.

Du point de vue de la protection des données, ce type de site peut poser deux sortes de problèmes. Premièrement, rien ne garantit que le médecin concerné sache qu'il est soumis à une évaluation. En second lieu, l'anonymat des évaluations est problématique, puisque rien ne garantit que les critiques figurant sur le site soient fondées sur l'expérience directe et personnelle d'un patient.

2.3 Évaluation de cours dans les hautes écoles

Les sites d'évaluation de cours dans les hautes écoles se rattachent aux évaluations d'enseignants et de professeurs. Ils permettent à des utilisateurs qui se sont préalablement enregistrés d'évaluer des cours ou des enseignants sur une échelle allant de «très mauvais» à «très bon» selon différents critères (impartialité, soutien, support du cours, intelligibilité, amusement, intérêt, rapport entre le travail fourni et la note obtenue). L'utilisateur publie lui-même le cours (et parfois l'enseignant) à évaluer. Il a en outre la possibilité de recommander le cours et de laisser un commentaire.

Le nom de l'enseignant peut être donné par la personne concernée ou par de simples utilisateurs de la plateforme. Même si les évaluations sont réservées aux personnes enregistrées sur le site, rien ne les empêche d'évaluer un cours qu'elles n'ont jamais suivi.

Du point de vue de la protection des données, le fait que tout utilisateur enregistré puisse introduire un cours sur le site pose problème. Des cours sont en effet susceptibles d'être évalués à l'insu de l'enseignant, ce qui va à l'encontre du principe voulant que toute collecte de données soit reconnaissable. En outre, les utilisateurs peuvent évaluer des cours qu'ils n'ont jamais suivis ou se montrer particulièrement critiques pour des raisons personnelles. Enfin, si les utilisateurs doivent s'enregistrer pour accéder au site, rien ne les empêche d'utiliser à cette fin une adresse électronique anonyme: en tel cas, même si l'administrateur du site l'interdit, l'évaluation sera de fait anonyme.

3 Problématique et risques

Problématique sous l'angle de la protection des données

Selon l'art. 3, let. e, de la loi fédérale sur la protection des données (LPD; RS 235.1), toute publication de données personnelles sur un site Internet constitue un traitement de données. Que l'administrateur de la plateforme d'évaluation ait traité lui-même ces données ou que le traitement soit le fait d'un de ses collaborateurs ou d'un tiers ne joue aucun rôle: l'administrateur fixant le cadre du traitement des données et exerçant de ce fait une influence déterminante sur leur évaluation et la présentation des résultats, il en est responsable. Il est en outre considéré comme le maître du fichier, conformément à l'art. 3, let. i, LPD, puisqu'il décide du but et du contenu de celui-ci. Il lui incombe donc de vérifier si les principes du traitement des données, en particulier

son caractère reconnaissable (art. 4, al. 4, LPD), sont respectés. La personne concernée par le traitement des données doit en outre avoir donné son consentement, sauf intérêt prépondérant d'ordre public ou privé ou exception prévue par la loi (art. 13 LPD). Aucun de ces motifs ne s'appliquant aux sites d'évaluation, le consentement de la personne concernée par l'évaluation est en principe nécessaire.

Problématique sous l'angle de la protection de la personnalité

La question de la protection de la personnalité sur les sites d'évaluation implique de mettre en balance la liberté d'expression avec les droits de la personnalité de la personne concernée par l'évaluation.

On distingue dans le domaine de la liberté d'expression les allégations de faits et les jugements de valeur. Devant correspondre à la vérité et étant susceptibles d'être prouvées, les premières sont présumées non attentatoires à la personnalité. Cependant, si les faits allégués ne sont pas notoires et que leur contenu est sensible, leur publication peut constituer une atteinte à la sphère privée.

Les jugements de valeur sont au contraire des points de vue ou des conclusions personnels exprimés sur une personne en particulier ou sur tel ou tel fait. Selon une jurisprudence constante du Tribunal fédéral, les jugements de valeur sont licites pour autant qu'ils semblent défendables et ne soient pas inutilement dénigrants ou offensants.

Les résultats publiés sur les sites d'évaluation autonomes contiennent le plus souvent des jugements de valeur. Généralement, en effet, la collecte des données ne satisfait pas aux méthodes statistiques reconnues (ni du point de vue quantitatif ni du point de vue qualitatif) et les personnes procédant aux évaluations ne sont pas suffisamment proches de l'élément évalué pour que les résultats puissent être qualifiés d'allégations de faits. Dès lors, si les résultats de l'évaluation portent atteinte à la personnalité, l'administrateur du site doit en répondre.

3.1 Risques encourus par les administrateurs

Les risques d'infraction à la protection des données encourus par les administrateurs varient en fonction du type de plateforme d'évaluation. Ces risques peuvent être décrits en s'appuyant sur les catégories dégagées dans les tableaux 1 et 2 ci-dessus et sur le type d'évaluation (quantitative, qualitative ou spécifique).

Problèmes de reconnaissance ou de consentement

L'art. 4, al. 4, LPD dispose que «[l]a collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée», afin que cette dernière puisse identifier à temps les atteintes à la personnalité induites par le traitement des données. L'administrateur d'une plateforme d'évaluation doit donc veiller à ce qu'elle puisse reconnaître immédiatement que des données la concernant sont traitées.

Lorsque la personne concernée a publié elle-même les informations à évaluer, l'administrateur de la plateforme peut présumer qu'elle a consenti au traitement des données. En revanche, lorsque ces informations ont été publiées par l'administrateur ou un utilisateur de la plateforme, elle ne peut reconnaître immédiatement que des données la concernant sont traitées. Dans ce dernier cas, si l'administrateur de la plateforme n'informe pas la personne concernée et n'obtient pas son consentement, il porte atteinte à sa personnalité aux termes de l'art. 12, al. 2, let. a (en relation avec l'art. 4, al. 4) et b, LPD. Si le traitement porte sur des données sensibles ou des profils de la personnalité, le consentement doit être exprès (art. 4, al. 5, LPD). Dans les autres cas, le consentement peut être implicite, pour autant que la personne concernée ait été informée de manière appropriée et ait consenti librement au traitement des données.

130 *Atteinte à la personnalité*

Comme vu plus haut, les évaluations se déroulant sur des plateformes en ligne doivent en général être qualifiées de jugements de valeur et ne doivent pas être inutilement dénigrantes ou offensantes. En principe, l'administrateur du site ne procède pas lui-même aux évaluations et il les synthétise automatiquement. Il n'est donc pas en mesure de juger si les résultats présentés sur son site sont inutilement dénigrants ou offensants (p. ex. lorsque des évaluations injustes faussent les résultats). Dès lors, moins une évaluation est significative du point de vue statistique et plus la distance entre l'objet évalué et celui qui l'évalue est importante, plus le risque d'atteinte à la personnalité est élevé.

Des commentaires inutilement dénigrants ou offensants publiés sur le site peuvent également constituer des atteintes à la personnalité. L'administrateur doit donc prendre suffisamment de mesures préventives pour effacer immédiatement de tels commentaires.

Les risques d'atteinte à la personnalité augmentent lorsque les évaluations peuvent être anonymes. Lorsque les utilisateurs doivent s'enregistrer, le risque est moindre mais il subsiste, car il est généralement possible d'utiliser une fausse adresse électronique.

3.2 Risques encourus par les personnes évaluées

La personne concernée par une évaluation peut subir une atteinte à sa personnalité, notamment lorsque les résultats de l'évaluation donnent une fausse image d'elle ou lorsque des utilisateurs faussent systématiquement leurs évaluations. Le risque de faire l'objet de fausses allégations est plus grand lorsque:

1. le nombre d'évaluations est réduit (manque de signification statistique),
2. la personne procédant à l'évaluation est peu qualifiée (manque de compétence),
3. la personne procédant à l'évaluation a un rapport distant avec l'objet évalué (manque de proximité).

Le risque de faire l'objet d'une évaluation faussée dépend donc de la conception de la plateforme. Par exemple, si les évaluations peuvent être anonymes, un utilisateur qui ne dispose ni des compétences ni des informations nécessaires pourra procéder à l'évaluation. En outre, si la plateforme publie les résultats dès qu'un petit nombre d'évaluations ont été faites, le risque d'une évaluation systématiquement faussée augmente.

3.3 Risques encourus par les personnes procédant aux évaluations

Les utilisateurs d'une plateforme d'évaluation doivent être conscients que, lorsqu'ils procèdent à une évaluation, ils rendent le plus souvent une sorte de jugement de valeur et que celui-ci ne doit pas être inutilement dénigrant ou offensant. Dans ce dernier cas, une plainte pour atteinte à la personnalité peut être déposée contre eux, voire une plainte pénale pour atteinte à l'honneur.

Si l'utilisateur peut rester anonyme, le risque de faire l'objet d'une plainte est minime. Rappelons toutefois que, en théorie, toute personne ayant procédé à une évaluation sur une plateforme en ligne peut être identifiée par son adresse IP.

4 Mesures et recommandations

De manière générale, les administrateurs devraient concevoir leurs plateformes d'évaluation de manière à minimiser les risques d'infraction à la protection des données ou les risques d'atteinte à la personnalité. En cas de risque d'atteinte à la personnalité, tant l'administrateur que la personne concernée doivent agir rapidement pour éviter ou limiter les dommages pour toutes les parties. On trouvera ci-dessous un catalogue des mesures que peuvent prendre les administrateurs, les personnes évaluées et les utilisateurs des plateformes d'évaluation pour se conformer aux dispositions sur la protection des données.

4.1 Administrateurs de plateforme d'évaluation

De manière générale, l'administrateur doit concevoir son site de manière à empêcher autant que possible toute atteinte à la personnalité. Les mesures concrètes varieront en fonction du type de plateforme (cf. tableaux 1 et 2).

4.1.1 La personne concernée publie elle-même l'objet de l'évaluation et l'autorise

132 Lorsque la personne concernée télécharge un élément sur un site en ligne et autorise les utilisateurs à l'évaluer, l'évaluation a lieu avec le consentement de la personne concernée. L'administrateur du site doit alors uniquement veiller à ce que les utilisateurs ne publient pas de propos dénigrants ou offensants. Si un tel abus lui est signalé, il doit immédiatement y mettre fin.

4.1.2 Un tiers publie l'objet de l'évaluation

Lorsque l'objet de l'évaluation (lié à une personne) peut être publié par l'administrateur ou un utilisateur du site, l'évaluation n'est pas immédiatement reconnaissable pour la personne concernée et se déroule sans son consentement. L'administrateur doit donc informer la personne concernée avant de procéder à l'évaluation et (à moins qu'il ne dispose d'un motif suffisant pour passer outre) obtenir son consentement.

4.1.3 Les évaluations peuvent être anonymes

Lorsque les évaluations peuvent être anonymes, la collecte des données est soumise à des conditions supplémentaires. Les informations obtenues dans ce type d'évaluation ne sont en effet exploitables que si les résultats sont robustes et significatifs du point de vue statistique, ce qui implique de récolter un grand nombre d'évaluations indépendantes. En outre, les utilisateurs procédant à l'évaluation doivent posséder une certaine proximité par rapport à l'élément évalué. L'administrateur du site doit donc veiller à ce que les résultats ne soient publiés que sur la base d'un nombre suffisamment élevé d'évaluations et que celles-ci aient été faites par des personnes qui connaissent l'objet de l'évaluation (p. ex. parce que l'image à évaluer s'est affichée sur leur écran).

De manière générale, les évaluations anonymes portant sur des personnes requièrent la plus grande prudence en raison des risques d'atteinte à la personnalité.

4.1.4 Les tiers doivent s'enregistrer pour évaluer l'objet

En principe, si une personne a dû s'enregistrer avant de procéder à une évaluation, elle n'est plus anonyme, à moins d'avoir utilisé un faux nom. L'administrateur du site doit donc prendre des mesures qui limitent au maximum les risques d'enregistrement anonyme, afin de minimiser les risques d'atteinte à la personnalité.

Il est vrai que rien n'empêche un utilisateur enregistré sous son vrai nom d'évaluer un objet qu'il ne connaît pas. En cas de litige, il pourra toutefois être identifié et des mesures pourront être prises contre lui.

4.1.5 La personne concernée autorise l'utilisateur à évaluer l'objet

Si la plateforme est conçue de telle sorte que l'utilisateur ne peut évaluer l'objet que si la personne concernée l'y autorise, cette mesure suffit.

Toutefois, si un abus est signalé à l'administrateur du site (commentaire offensant d'un utilisateur), celui-ci doit immédiatement y mettre fin.