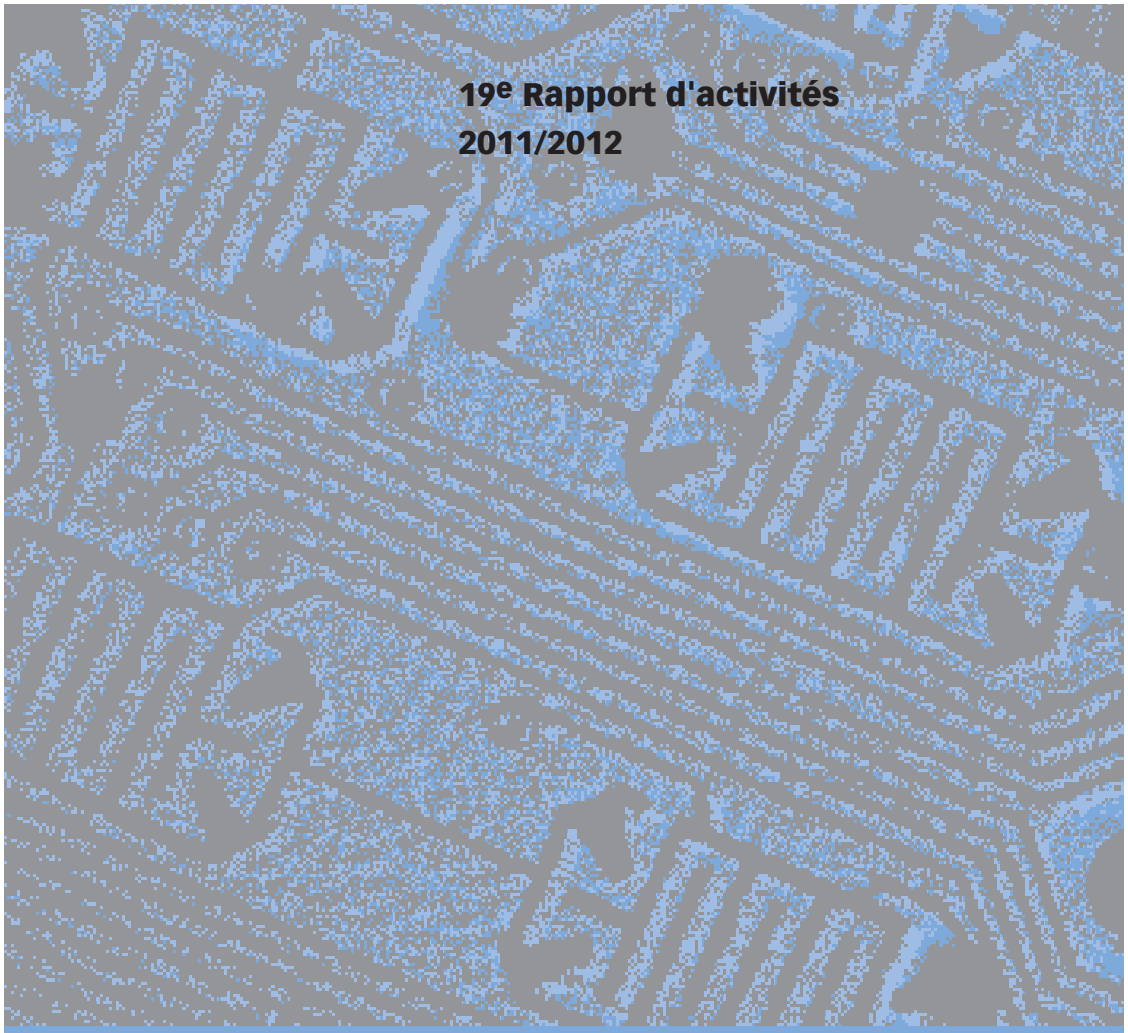


19e Rapport d'activités 2011/2012

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2011/2012 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 à l'Assemblée fédérale un rapport sur son activité (art. 30 LPD). Le présent rapport couvre la période du 1er avril 2011 au 31 mars 2012.

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. 410.019.d/f

Table des matières

Avant-propos – Bilan et perspectives

Des améliorations considérables ont été réalisées l'année passée dans le domaine de la protection de l'Etat. Au cours de la session de décembre 2011, à l'occasion de la révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI), le Parlement a adopté une modification découlant du message que nous n'avons eu de cesse d'exprimer: le droit d'accès indirect affaiblit les droits des citoyens et ne résisterait très probablement pas à un examen de la Cour européenne des droits de l'homme. Désormais, c'est le droit d'accès direct conformément aux art. 8 et 9 de la loi fédérale sur la protection des données (LPD) qui est en principe applicable; celui-ci peut toutefois être différé si des intérêts prépondérants l'exigent. Dans ce cas, la personne ayant requis l'accès à des données la concernant peut demander qu'un examen soit effectué par le PFPDT qui, en cas d'erreurs, peut émettre une recommandation.

Aucune demande de référendum n'ayant été déposée contre cette modification, le Conseil fédéral devrait fixer l'entrée en vigueur de cette modification de loi pour le début du mois de juillet 2012. En parallèle, suite à un recours, le Tribunal fédéral s'est penché sur la réglementation établie actuellement à l'art. 18 LMSI et a, pour la première fois examiné la conformité de cette disposition avec les exigences de la Convention européenne des droits de l'homme (CEDH) dans un arrêt rendu le 2 novembre 2011. Cet arrêt a amélioré considérablement le statut juridique des personnes concernées. La cour suprême helvétique a établi qu'un droit d'accès indirect était conforme à la CEDH tant que les intérêts de la protection de l'Etat le justifiaient. Néanmoins, contrairement au libellé de la disposition, les juges fédéraux ont exigé qu'en cas d'erreurs, le PFPDT puisse émettre non seulement des recommandations, mais aussi des instructions contraignantes. Selon eux, c'est le seul moyen pour que le mécanisme de contrôle exercé par le PFPDT et le Président de la Cour du Tribunal administratif fédéral soit véritablement efficace et réponde aux exigences d'un contrôle indépendant des traitements de données effectués par les organes de protection de l'Etat. À l'avenir, le nouvel art. 18 LMSI permettra explicitement au Tribunal administratif fédéral d'ordonner que ces derniers remédient aux erreurs. Nous partons du principe qu'à l'entrée en vigueur de la nouvelle LMSI, l'arrêt du Tribunal fédéral sera toujours valable et que de ce fait, les recommandations du PFPDT devront avoir un caractère contraignant.

Comme en 2010, la formation des jeunes a été un point fort de notre action et nous avons poursuivi nos efforts tout au long de l'année. En effet, nous sommes persuadés qu'à l'ère des réseaux sociaux, la sensibilisation des jeunes utilisateurs requiert des initiatives particulières et nous ne voulons pas nous contenter de lancer des appels aux écoles et aux parents. Nous sommes donc à la recherche de partenariats, notamment et aussi en raison des limites de nos moyens. Le projet NetLa, lancé en 2011

en collaboration avec le Conseil pour la protection de la sphère privée, a aussi été porté à la connaissance d'un grand nombre d'écoliers. Pour le seul mois de novembre, dernier mois de la campagne, 6000 internautes ont cliqué 225'000 fois pour visiter le portail mutimédia. Nous avons également mis au point un matériel d'enseignement sous forme de leçons afin de sensibiliser les jeunes adultes à la sécurité des données lorsqu'ils utilisent les nouveaux médias. Ces leçons sont disponibles gratuitement en ligne sur Internet et sont ciblées sur les élèves de l'enseignement secondaire supérieur. Par ailleurs, nous avons collaboré à des cours de formation organisés par les universités de Neuchâtel et de Lausanne. Nous avons en outre développé le service interactif Thinkdata.ch en collaboration avec l'autorité de protection des données du canton de Genève, l'Université de Genève, l'Observatoire technologique de l'Etat de Genève, l'IDHEAP Lausanne ainsi que d'autres acteurs. Ce site en français – bientôt disponible en allemand – offre sous forme de scénarios des réponses précises et concises à toutes les personnes qui s'intéressent à la protection des données et à la transparence ou qui y sont directement confrontées. Nous sommes actuellement à la recherche de moyens financiers afin d'élargir notre offre et de la mettre en ligne dans d'autres langues. Enfin, pour la quatrième fois, nous avons organisé la Journée suisse du droit de la protection des données avec les universités de Berne, Neuchâtel et Fribourg.

2011 a également été une année jalonnée de nombreux contrôles et d'établissements des faits. Ainsi, nous avons examiné le système de surveillance vidéo auprès de cinq entreprises de transports publics et proposé un certain nombre d'améliorations qui ont été acceptées. Dans le cadre de la mise en œuvre de l'accord de Schengen, nous avons procédé à une visite de contrôle auprès de l'ambassade de Suisse à Moscou et émis diverses recommandations. Nous avons également achevé avec succès deux procédures d'établissement des faits, l'une auprès d'un club de tennis disposant d'un système de réservation basé sur la reconnaissance biométrique, la seconde concernant le traitement de données sur la solvabilité. Nous avons clos le dossier relatif à la plateforme d'informations «Car Claims Information Pool», gérée par les assureurs, et suggéré diverses améliorations. Citons encore les différentes modifications que nous avons proposées à un prestataire de services dans le domaine des manifestations de sport amateur; nous demeurons en contact avec lui à propos de la mise en œuvre des mesures en question. Enfin, nous avons introduit une procédure d'examen des faits concernant un nouveau jeu informatique qui transmet de manière illicite au fabricant des données concernant les ordinateurs des utilisateurs.

Parmi les nombreuses consultations des offices, je citerai en particulier celle concernant la révision de la loi fédérale et de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication. À cet égard, nous avons obtenu la création d'une base légale sur laquelle reposera l'utilisation de programmes de type «GovWare».

Lors de l'élaboration de ce type de bases légales en vue de la surveillance de l'utilisation de l'infrastructure électronique au sein de l´administration fédérale, nous avons également attiré l'attention sur la nécessité d'une réglementation claire concernant l'enregistrement, la conservation, mais aussi l'analyse des données secondaires générées par les communications. Dans le cadre de la révision de loi touchant le système tarifaire SwissDRG, nous avons contacté les différents acteurs concernés et exigé que les assurances ne reçoivent que les données dont elles ont vraiment besoin. De plus, à l'occasion de la révision totale de la loi sur le contrat d'assurance, nous avons souligné l'importance d'inscrire dans la loi l'institution du médecin-conseil.

Parmi les publications parues sur notre site Internet durant l'année sous revue, énumérées au chiffre 3.3, nous mentionnerons en particulier nos commentaires explicatifs concernant la directive de l'Union européenne «Vie privée et communication électronique» et ceux concernant l'informatique en nuage (cloud computing) en tant que mode de traitement de données.

En 2011, la situation a également évolué dans le domaine du principe de la transparence. Le nombre des demandes d'accès adressées à l'administration fédérale a presque doublé et 65 demandes en médiation nous ont été transmises. Nous avons mené à bien 30 procédures de médiation et dans la grande majorité des cas, nous sommes parvenus à une solution plus favorable pour le demandeur. Toutes les recommandations sont résumées au chiffre 2.3.1 et peuvent être consultées sur notre site Internet. Suite à des recours, le Tribunal administratif fédéral a dû se pencher sur quatre de nos recommandations et a soutenu nos argumentations. En outre, dans le cadre de la révision de la loi sur les cartels, nous avons obtenu que les autorités en matière de concurrence ne soient pas soustraites du champ d'application de la loi sur la transparence.

Nous pouvons dire d'ores et déjà que divers thèmes vont continuer à nous occuper durant l'année à venir. Citons entre autres la requête politiquement très délicate émise par les États-Unis visant à découvrir, dans le cadre d'une procédure «hit/no hit», si une personne déterminée est enregistrée avec son empreinte digitale ou son ADN dans les banques de données suisses Codis ou Afis. Au cours des négociations, il sera important de veiller à ce que les personnes concernées qui figurent à tort dans ces deux banques de données se voient accorder les mêmes droits aux États-Unis qu'en Suisse. Il ne sera pas facile d'obtenir cette garantie car à notre avis, les États-Unis ne disposent en principe pas d'une protection des données suffisante. C'est pourquoi l'appréciation dans le cas d'espèce ne doit pas être effectuée par un «privacy officer» dépendant de l'administration, mais par une autorité judiciaire indépendante. Il est en outre important que dans tous les cas où une concordance des données est constatée, la suite de la procédure se déroule dans le cadre de la procédure d'entraide judiciaire

fixée par une loi. En d'autres termes, les conditions de communication de données personnelles doivent être examinées dans chaque cas d'espèce sur la base des accords en vigueur; les automatismes doivent être exclus. Il va également de soi que ce type d'échange doit être limité aux formes graves de criminalité et que la Suisse doit bénéficier d'un droit de réciprocité.

Les réseaux sociaux vont continuer à nous préoccuper, notamment la politique commerciale de Facebook. Nul n'ignore que l'objectif de ce dernier est d'accéder à un maximum d'informations sur ses utilisateurs et de générer des profils de la personnalité à des fins publicitaires. L'entreprise réalise ainsi un chiffre d'affaire de plusieurs milliards et modifie sans cesse les conditions générales d'utilisation, au détriment des utilisateurs et sans demander leur consentement. Depuis peu, non seulement les personnes qui sont sur Facebook, mais aussi celles qui ne l'utilisent pas en sont la cible. Dans le projet des conditions d'utilisation de mars 2012, on peut lire que celles-ci sont aussi applicables aux «non-utilisateurs qui interagissent avec Facebook en dehors des États-Unis». Autrement dit, ces «non-utilisateurs» sont réputés consentir à la transmission et au traitement de leurs données aux États-Unis, ce qui englobe aussi le traitement à des fins publicitaires. Le scandale dans cette histoire est que la plupart des «non-utilisateurs» ne savent absolument pas qu'ils «interagissent» avec Facebook. Comment est-ce possible? Sur bon nombre de sites Internet se trouve la petite icône «J'aime» qui est lié à Facebook (reconnaissable p. ex. à la lettre en minuscule «f»). La visite de l'utilisateur sur la page consultée est automatiquement communiquée à Facebook, ceci même s'il n'a pas cliqué sur l'icône «J'aime». Ce système permet donc d'établir des profils de la personnalité très précis aussi sur les personnes qui se refusent à utiliser Facebook. Nous allons concentrer nos efforts pour obtenir des exploitants de sites qu'ils donnent à leurs visiteurs la possibilité de décider s'ils consentent à ce type de transmission ou non. Rien d'étonnant à ce qu'entre-temps, une certaine défiance ait également vu le jour au niveau parlementaire. La conseillère nationale valaisanne Viola Amherd a déposé en septembre 2011 un postulat dans lequel elle enjoint le Conseil fédéral d'examiner l'état actuel de la législation sur les médias sociaux, de dire quelles sont les lacunes du droit et de se prononcer sur la nécessité de créer une loi proprement dite sur les médias sociaux. Il est notamment mentionné dans le développement du postulat que «les médias sociaux apportent une dimension nouvelle dans la communication et l'utilisation des médias, qui menace de remettre en cause l'application des lois nationales et des valeurs-clés». Cela se passe de commentaires!

Dans le domaine des droits d'auteur, l'arrêt du Tribunal fédéral en la cause Logistep a fait bouger les choses. Tout d'abord un bref rappel: le Tribunal fédéral a considéré que les recherches d'adresses IP effectuées secrètement par Logistep dans le but d'intenter une action civile contre des utilisateurs soupçonnés de violer les droits d'auteur

n'étaient pas licites. Cet arrêt a provoqué un certain émoi auprès des détenteurs de droits. Dans son rapport de gestion 2010, le Tribunal fédéral a fait observer que la situation actuelle était insatisfaisante sous l'angle juridique et qu'il appartenait au législateur de prendre les mesures nécessaires pour assurer une protection des droits d'auteurs appropriée aux nouvelles technologies. À ce jour, cette initiative remarquable et inhabituelle de notre cour suprême n'a suscité aucune réaction de la part du Conseil fédéral. Des interventions parlementaires demandant une amélioration de la situation ont entre-temps été déposées au Parlement. Nul ne conteste que la protection des droits d'auteur est un thème très délicat et fait l'objet de vives discussions, pas seulement en Suisse (pour preuve, le succès du Parti Pirate allemand). La position qui était déjà la nôtre durant la procédure n'a pas changé: sur la base du droit en vigueur, on ne peut utiliser une adresse IP que dans le but de déterminer, dans le cadre d'une procédure pénale, la personne qui a violé des droits d'auteur. Les actions civiles ne peuvent entrer en jeu qu'ensuite.

Le 9 décembre 2011, le Conseil fédéral a approuvé le rapport sur l'évaluation de la loi sur la protection des données et l'a soumis au Parlement. Outre la constatation positive que la loi sur la protection des données avait permis d'atteindre un niveau de protection sensible dans les domaines où les défis étaient déjà connus au moment de son entrée en vigueur et que le PFPDT s'était avéré un instrument efficace pour améliorer la protection offerte par la loi, ce rapport n'en souligne pas moins clairement la nécessité d'agir:

«De l'avis du Conseil fédéral, la révision de la LPD devrait avoir pour objectif principal d'adapter la loi aux développements technologiques et sociétaux intervenus depuis son entrée en vigueur. C'est pourquoi il entend axer sa réflexion sur les quatre problématiques centrales liées aux évolutions technologiques et sociétales en cours, soit 1. l'accroissement du volume des données traitées; 2. les traitements de données difficiles à reconnaître comme tels, aussi bien pour les intéressés que pour le PFPDT; 3. l'internationalisation croissante des traitements de données; 4. la difficulté toujours plus marquée à garder le contrôle de données une fois qu'elles ont été rendues publiques. Dans ce contexte, le Conseil fédéral souhaite examiner quelles mesures lui permettraient d'atteindre en particulier les objectifs suivants:

- Assurer la protection des données plus en amont: une réflexion globale doit permettre de détecter les éventuels problèmes et d'y remédier dès la phase de conception des nouvelles technologies. L'idée est d'éviter que l'on se contente de corriger des problèmes après coup, avec des programmes de correction (approfondissement de la notion de protection intégrée de la vie privée ou «privacy by design»). Il importe également de favoriser les technologies respectueuses de la protection des données.

- Sensibiliser davantage les personnes concernées: les personnes concernées doivent être plus au fait des risques que représentent les nouvelles technologies pour la protection de la personnalité.
- Améliorer la transparence: il convient d'améliorer la transparence des traitements de données, notamment dans les nouveaux contextes complexes dans lesquels ni les personnes concernées ni le PFPDT ne peuvent les identifier facilement. On veillera ce faisant à ne pas submerger les personnes concernées d'informations.
- Améliorer le contrôle et la maîtrise des données: le contrôle et la maîtrise des données après leur divulgation est un aspect primordial. Ainsi, la possibilité de renforcer les mécanismes de contrôle à disposition du PFPDT et d'adapter aux développements technologiques les droits des personnes concernées devrait être analysée. On examinera par exemple dans ce cadre un renforcement des voies de droit collectives ainsi qu'une précision du droit à l'oubli.
- Protéger les mineurs: il faut tenir compte du fait que les mineurs ont une conscience moindre des risques et conséquences inhérents au traitement de données à caractère personnel.»

Le Conseil fédéral entend en outre examiner si et dans quelle mesure il est souhaitable de renforcer l'indépendance du PFPDT. Il s'intéressera également à la possibilité d'étendre l'instrument de l'autorégulation, en incitant par exemple les organisations sectorielles à élaborer des «règles de bonne pratique» qui seraient ensuite approuvées par le PFPDT.

Ces visées exprimées par le Conseil fédéral sont les nôtres depuis des années et nous sommes très heureux que la nécessité d'agir soit désormais reconnue à ce niveau. Cela dit, le souhait exprimé par le Conseil fédéral d'attendre les résultats des réformes en cours dans l'Union européenne nous cause un certain souci. Bien entendu, tout projet de réforme suisse doit être coordonné aux mesures prises au niveau européen. Mais cela ne doit pas empêcher le gouvernement de créer en parallèle un groupe d'experts qui examinera la problématique du point de vue suisse. En matière de protection des données, notre pays doit aussi avoir l'ambition d'élaborer ses propres solutions au lieu de se cantonner à l'adaptation autonome au droit européen.

Hanspeter Thür

Répertoire des abréviations

ACC	Autorité de contrôle commune
AFAPDP	Association francophone des autorités de protection des données personnelles
AFC	Administration fédérale des contributions
ATF	Arrêt du Tribunal fédéral
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CDAS	Conférence des directrices et directeurs cantonaux des affaires sociales
CdC	Centrale de compensation
CDF	Contrôle fédéral des finances
CDI	Conventions contre les doubles impositions
CDS	Conférence suisse des directrices et directeurs cantonaux de la santé
ChF	Chancellerie fédérale
CFV	Commission fédérale pour les vaccinations
CSN	Commission fédérale de sécurité nucléaire
COMCO	Commission de la concurrence
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFE	Département fédéral de l'économie
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DRG	Diagnoses Related Groups

ESPA	Enquête suisse sur la population active
EVA	Etablissement électronique de visas
FATCA	Foreign Account Tax Compliance Act
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
GEWA	Système de traitement des données en matière de lutte contre le blanchiment d'argent
ISAS	Système d'information sécurité extérieure
IFSN	Inspection fédérale de la sécurité nucléaire
ISIS	Système de traitement des données relatives à la protection de l'Etat
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
LAA	Loi fédérale sur l'assurance-accidents
LAMal	Loi fédérale sur l'assurance-maladie
LCA	Loi fédérale sur le contrat d'assurance
LCD	Loi sur la concurrence déloyale
LHR	Loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes
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
LPers	Loi fédérale sur le personnel de la Confédération
LPGA	Loi fédérale sur la partie générale du droit des assurances sociales
LPP	Loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité

LSIP	Loi fédérale sur les systèmes d'information de police de la Confédération
LTC	Loi sur les télécommunications
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
N-SIS	Partie nationale du Système d'information Schengen
NAVS13	Numéro AVS à 13 chiffres
OAC	Ordonnance réglant l'admission des personnes et des véhicules à la circulation routière
OAccD	Ordonnance sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement et d'homologation
OACDI	Ordonnance relative à l'assistance administrative d'après les conventions contre les doubles impositions
OAMal	Ordonnance sur l'assurance-maladie
OCDE	Organisation pour la coopération et le développement économiques
ODM	Office fédéral des migrations
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFC	Office fédéral de la culture
OFEN	Office fédéral de l'énergie
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
OFT	Office fédéral des transports
OFJ	Office fédéral de la justice

OFPP	Office fédéral de la protection de la population
OFSP	Office fédéral de la santé publique
OLPD	Ordonnance relative à la loi fédérale sur la protection des données
OPrI	Ordonnance concernant la protection des informations de la Confédération
OSCPT	Ordonnance sur la surveillance par poste et télécommunication
OSI-SRC	Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération
OST	Ordonnance sur les services de télécommunication
OTrans	Ordonnance sur le principe de la transparence dans l'administration
OTVA	Ordonnance régissant la taxe sur la valeur ajoutée
PEP	Policy Enforcement Point
PFPDT	Préposé fédéral à la protection des données et à la transparence
PKI	Public Key Infrastructure
SECO	Secrétariat d'Etat à l'économie
SIS	Système d'information Schengen
SRC	Service de renseignements de la Confédération
SYMIC	Système d'information central sur la migration
Swissmedic	Institut suisse des produits thérapeutique
TAF	Tribunal administratif fédéral
UPI	Unique Person Identification
VBZ	Verkehrsbetriebe Zürich (Transports de la ville de Zurich)
VIS	Système d'information sur les visas
ZVV	Verkehrsverbund des Kantons Zürich (Communauté des transports publics du canton de Zurich)

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Externalisation dans le cadre du recensement de la population

Suite à notre intervention, la lettre envoyée par l'Office fédéral de la statistique pour demander aux personnes de participer à ses enquêtes informe désormais de manière transparente sur le caractère volontaire de la participation à l'enquête. Des progrès ont également été accomplis dans le domaine de l'assurance qualité par l'entreprise mandatée pour effectuer l'enquête.

Dans notre 18e rapport d'activités 2010/2011, au chiffre 1.1.1, nous avons rendu compte de nos contrôles portant sur les traitements de données et les flux d'informations dans le cadre du recensement de la population. Entretemps, la partie du contrôle qui concerne l'Office fédéral de la statistique (OFS) a pratiquement pu être menée à terme. Suite à notre critique, l'OFS améliore le contenu de l'information transmise dans la lettre invitant les citoyens à participer à une enquête. Jusqu'ici, cette lettre ne contenait pas d'informations claires sur une éventuelle obligation de participer, afin de ne pas influencer négativement le taux de réponse. Durant l'année écoulée, l'OFS a testé diverses formes d'informations plus transparentes et nous a ensuite soumis une proposition acceptable: dorénavant toute lettre annonçant l'enquête sera accompagnée d'un petit dépliant (Leporello). Le but de ce dépliant est d'informer clairement sur l'obligation de participer. Nous vérifierons l'application de cette amélioration sur la base de quelques cas concrets. À notre avis, des informations adéquates sur le caractère volontaire ou obligatoire de la participation sont requises pour toutes les enquêtes menées par l'OFS.

Un autre aspect sur lequel nous ne sommes pas encore tombés d'accord concerne le contrôle des employés de l'institution privée qui réalise l'enquête. Nous considérons le contrôle de qualité, tel qu'il est pratiqué jusqu'ici, comme étant disproportionné. Pour l'instant, nos arguments n'ont pourtant pas réussi à convaincre l'entreprise concernée. Celle-ci a relevé que la pratique qu'elle a développée est largement répandue dans la branche et qu'un déroulement différent du contrôle de la qualité n'était pas en mesure de répondre aux exigences du mandant (en l'occurrence l'OFS). Nos recherches ont abouti à un constat similaire. Toutefois, le fait qu'une certaine pratique soit très répandue ne justifie en aucun cas un traitement de données illicite.

Nous aimerions, en collaboration avec cette entreprise, trouver une solution qui puisse servir de solution modèle pour la branche. Cette solution doit tenir compte du progrès

technique et de la baisse constante du prix des supports de stockage – le prix permettant aujourd'hui un enregistrement audio de l'ensemble du matériel lié à l'enquête. Nous nous sommes entretemps mis d'accord avec l'entreprise concernée sur la démarche à adopter. Celle-ci nous soumettra pour examen un concept d'assurance qualité qui prend en compte les exigences de la protection des données, et nous accompagnerons sa mise en œuvre. Nous poursuivrons notre contrôle dans ce domaine et continuerons à en informer le public.

1.1.2 Demandes de citoyens concernant les enquêtes statistiques

Nous recensons ces derniers temps une augmentation du nombre de questions de citoyens relatives aux enquêtes statistiques. Ces questions portent principalement sur la proportionnalité des évaluations, sur l'utilisation du numéro AVS dans la statistique et sur l'obligation de répondre. Nous avons donc poursuivi nos activités dans ce domaine.

De manière générale, nous constatons que le nombre de demandes des citoyens relevant de la statistique n'a cessé de croître ces deux dernières années. Ce sont trois domaines principaux qui préoccupent les citoyens:

- L'envergure du questionnaire: la critique la plus fréquente est qu'il comporte trop de questions et que celles-ci font trop fortement intrusion dans la sphère privée. Pour chaque enquête, l'Office fédéral de la statistique (OFS) publie une profusion d'informations, parfois même le questionnaire. Si ce n'est pas le cas, nous pouvons sur demande y avoir accès. Notre rôle dans ce domaine se limite cependant à vérifier le caractère plausible des questions.
- Utilisation du numéro AVS: pour les personnes concernées, il existe une contradiction entre l'identification exacte de la personne interrogée et le but non personnel d'une collecte de données personnelles dans la statistique. En plus du conseil donné aux personnes concernées, nous nous sommes engagés pour des règles plus claires dans le domaine de la législation (cf. ch. 1.1.3 du présent rapport d'activités).
- Obligation de fournir une réponse: c'est la raison la plus fréquente pour laquelle les citoyens et citoyennes nous contactent. À ce jour, l'obligation de répondre n'existe que pour l'Enquête suisse sur la population active (ESPA) et l'enquête structurelle (dans le cadre du recensement de la population). Une initiative parlementaire vise à supprimer l'obligation de répondre pour l'enquête

ESPA. Nous avons œuvré dans le sens qu'à l'avenir l'OFS informe de manière plus transparente sur le caractère facultatif ou obligatoire de la participation à une enquête (cf. ch. 1.1.1 du présent rapport d'activités).

1.1.3 Utilisation du numéro AVS dans la statistique

Le numéro AVS joue un rôle important dans la statistique. Nous avons examiné de plus près les bases légales qui permettent son utilisation.

Avec l'exemple du projet de l'Office fédéral de la statistique (OFS) pour la modernisation de la statistique de la formation, nous avons étudié l'utilisation du numéro AVS de manière générale dans le domaine de la statistique. La question de savoir si les bases légales existantes sont suffisantes pour que l'OFS puisse exiger des écoles qu'elles leur livrent les numéros AVS ne faisait pas l'unanimité. Notre position initiale est décrite plus en détail au chiffre 1.1.3 de notre 18e rapport d'activités 2010/2011.

Dans notre prise de position, nous avions défendu l'avis que l'OFS dispose de bases légales suffisantes uniquement dans le cas des relevés indirects, basés sur la loi sur l'harmonisation des registres. L'OFS a mandaté une expertise à ce sujet dans laquelle l'expert mandaté parvient à la conclusion opposée.

Nous sommes conscients du fait que pour l'OFS le numéro AVS joue un rôle essentiel en tant qu'élément d'appariement indispensable. Lui seul permet, en qualité d'élément d'identification, d'établir des relations entre les différentes enquêtes. Afin de simplifier la situation juridique pour les participants à une enquête, situation déjà compliquée même aux yeux des experts en droit, nous nous sommes mis d'accord avec l'OFS sur le fait que celui-ci créera une nouvelle norme lors de la prochaine révision de la loi sur la statistique fédérale. Cette norme aura pour objectif de réglementer l'utilisation du numéro AVS pour l'ensemble du domaine de la statistique.

1.1.4 Aspects théoriques du nouveau numéro AVS

Le nouveau numéro AVS est entré en vigueur depuis 2008 et remplace progressivement l'ancien numéro AVS. Nous avons rencontré l'Office fédéral des assurances sociales et la Centrale de compensation pour comprendre comment ce nouveau numéro est attribué et utilisé et qui sont ses utilisateurs.

À partir de 2008, l'ancien numéro AVS à 11 chiffres a été progressivement remplacé par le nouveau numéro AVS à 13 chiffres (NAVS13). La Centrale de compensation (CdC) a effectué ce passage. Nous avons rencontré l'Office fédéral des assurances sociales

(OFAS) et la CdC qui nous ont expliqué le processus d'attribution de ce nouveau numéro, son utilisation et les problèmes qui subsistent.

Lors du passage de l'ancien au nouveau numéro AVS, les problèmes sont survenus dans deux situations particulières et distinctes. En effet, il arrive qu'une personne possède plusieurs numéros AVS ou alors que le même numéro soit attribué à plusieurs personnes. Dans le premier cas, la solution consiste à fusionner les numéros: un numéro est choisi et les autres sont désactivés – ils ne pourront plus être attribués. Dans le second cas, tous les numéros sont désactivés et de nouveaux numéros sont attribués aux différentes personnes.

À l'heure actuelle, 20 millions de personnes sont enregistrées dans UPI, le registre national de référence pour le NAVS13 géré par la CdC. La CdC estime que 1% des cas au maximum ont plus d'un numéro attribué, tandis que 10'000 à 20'000 personnes partagent un numéro identique. Ces derniers cas sont résorbés au fur et à mesure qu'ils sont découverts.

Ces cas problématiques proviennent d'erreurs humaines lors de l'épuration de l'ancien registre avant l'attribution des nouveaux numéros, mais également de difficultés techniques relatives aux communications électroniques entre les registres fédéraux et UPI. Ils peuvent aussi être imputés en partie à la qualité des registres qui fournissent les données au registre UPI.

Il est possible pour différentes organisations de s'annoncer comme utilisateur systématique du NAVS13 auprès de la CdC. Celle-ci ne peut refuser d'inscrire une organisation qui s'annonce comme utilisateur systématique. Toutefois, parallèlement à la publication de l'annonceur dans l'annuaire électronique disponible sur Internet, elle détermine si le statut d'utilisateur systématique est reconnu. Si l'utilisateur demande un accès au registre UPI ultérieurement, celui-ci lui sera accordé en fonction de sa légitimité en tant qu'utilisateur systématique.

La CdC met à disposition des utilisateurs systématiques des outils d'interrogation qui permettent de retrouver des données identitaires à partir d'un NAVS13 ou d'obtenir le NAVS13 d'une personne à partir de données identitaires. Il est également possible grâce à ces outils de vérifier la validité d'un NAVS13. Pour diminuer les risques d'erreurs lors des re-synchronisations, la CdC impose aux registres tiers de gérer le NAVS13 conjointement avec, au minimum, cinq autres champs de données: le nom, le prénom, la date de naissance, le sexe et la nationalité.

Nous avons constaté que la CdC est consciente des problèmes liés à l'unicité du numéro AVS et qu'elle ne recommande pas forcément l'utilisation de ce numéro dans tous les domaines (cf. ch. 1.3.12), en particulier dans des domaines très sensibles comme celui de la Cybersanté (eHealth).

1.1.5 Cas non recensés de violence des jeunes

Dans le cadre d'une consultation des offices, nous avons pris position sur la mise en place d'un relevé régulier au niveau national des cas non déclarés dans le domaine de la violence et de la criminalité chez les jeunes.

Dans le cadre d'une enquête nationale sur les cas non signalés de violence des jeunes, il était prévu d'interroger également des enfants âgés de dix ans. Nous avons pris position en critiquant d'une part l'absence de base légale pour une telle enquête; d'autre part, nous sommes d'avis que l'enquête doit être effectuée sur une base volontaire, ce qui veut dire que les participants doivent accepter de plein gré après avoir été préalablement informés. Un enfant peut le faire en conformité avec la loi pour autant qu'il soit capable de discernement en ce qui concerne l'objet du consentement. Compte tenu de la quantité et de la nature des données personnelles qui sont traitées dans l'enquête, nous avons toutefois défendu le point de vue que le consentement devait être obtenu non seulement de l'enfant interrogé, mais aussi de ses représentants légaux, à savoir ses parents. D'autre part, tout tiers (tel que parent ou autre proche), dont les données personnelles seraient traitées, devrait également être informé avant que celles-ci soient enregistrées.

1.1.6 Échange de données facilité entre les autorités fédérales et cantonales

En octobre 2007, un postulat chargeant le Conseil fédéral d'étudier les moyens de faciliter l'échange de données entre autorités fédérales et cantonales a été déposé au Conseil national. Un examen mené à grande échelle a démontré que l'on ne pouvait pas blâmer la protection des données pour les éventuelles difficultés au niveau de ces échanges.

Divers incidents, en particulier dans le domaine de l'assistance sociale, ont ces dernières années donné l'impression au public que les échanges de données entre les autorités fédérales et cantonales laissaient à désirer. À plusieurs reprises, on a suspecté une protection des données trop rigoureuse d'empêcher les échanges de données nécessaires dans les situations d'urgence. C'est dans ce contexte que le 5 octobre 2007 le conseiller national Lustenberger a déposé un postulat demandant de «faciliter l'échange de données entre autorités fédérales et cantonales». Ce dernier charge le Conseil fédéral d'examiner comment simplifier l'échange de données entre les autorités de la Confédération et celles des cantons. Le postulant a estimé que le risque d'abus était particulièrement élevé dans les domaines de l'assistance sociale, de la naturalisation, de la fiscalité et des assurances sociales. Il a donc également jugé

nécessaire de vérifier si la protection des données dans ces domaines constituait un obstacle à un échange efficace des données.

Le Conseil fédéral a mandaté le Département fédéral de justice et police (DFJP) de préparer le rapport. La responsabilité a été confiée à l'Office fédéral de la justice (OFJ), qui a mis sur pied un groupe de travail. Celui-ci était constitué d'un représentant de l'Office fédéral des assurances sociales (OFAS), de l'Administration fédérale des contributions (AFC), l'Office fédéral des migrations (ODM), l'Office fédéral de la police (fedpol), la Conférence des directrices et directeurs cantonaux des affaires sociales (CDAS), la Conférence des directeurs cantonaux de justice et police (CCDJP), et de chaque canton pour les domaines de la naturalisation, de la fiscalité et de la protection des données. Par ailleurs, nos spécialistes des divers domaines étaient également invités à ces réunions.

Au printemps 2009, l'OFJ a chargé le bureau Vatter AG d'examiner l'échange de données personnelles entre les autorités fédérales, cantonales et communales. L'étude a conclu que les échanges avaient lieu principalement entre les autorités cantonales et communales et que l'influence possible de la Confédération était donc restreinte. Le Conseil fédéral a pu prendre connaissance du fait que de manière générale le flux de données fonctionnait bien. Il repose sur des bases légales et n'est pas entravé par la protection des données. L'étude a également montré que les problèmes de collecte des données critiqués à l'origine n'avaient pas été causés par des dispositions de protection des données, mais plutôt par un manque de connaissances juridiques des autorités impliquées. Le rapport aboutit ainsi à la conclusion importante à nos yeux qu'une révision de la loi sur la protection des données n'est donc pas nécessaire.

L'enquête a également révélé des points faibles au niveau de l'échange de données entre les autorités. Le Conseil fédéral a dans les grandes lignes suivi les recommandations de l'étude. Par décision du 22 décembre 2010, il a alors transmis divers mandats d'examen au DFJP, au Département fédéral de l'intérieur (DFI) et au Département fédéral de l'économie (DFE). Fin novembre 2011, l'OFJ a résumé ces mandats ainsi que les résultats obtenus jusque-là dans le rapport «Faciliter l'échange de données entre autorités fédérales et cantonales». L'application du postulat Lustenberger nous a montré, en tant qu'accompagnateurs de cette intervention, que les efforts parfois importants qui doivent être fournis pour l'échange de données ne peuvent pas être imputés à la protection des données.

1.1.7 Thinkdata.ch – un outil de sensibilisation à la protection des données et à la transparence

Nous avons participé à un groupe de travail initié par ThinkServices à Genève. Ce groupe a développé un outil de sensibilisation à la protection des données et à la transparence à l'intention des organisations. Cet outil, élaboré en français, a été présenté à l'occasion de la 6e journée de la protection des données.

Contactés par l'autorité genevoise de protection des données et de transparence en janvier 2011, nous avons rejoint le groupe de travail «Documents, Société, Transparence» pour participer à ses travaux. Le groupe, composé de chercheurs de l'Université de Genève et de l'Université de Lausanne entre autres, d'autorités de protection des données cantonales et fédérales et d'indépendants, s'est réuni une fois par mois durant l'année 2011. L'objectif que le groupe s'est fixé rapidement était de produire un outil de sensibilisation à la protection des données et à la transparence à l'intention des organisations.

Par le biais des organisations en général, l'idée était de s'adresser plus spécifiquement aux différents acteurs de celles-ci, en fonction de leur métier. Ainsi quatre groupes ont été définis: les cadres, les responsables des ressources humaines, les responsables IT et les employés. L'outil présente sous l'angle des métiers mais également des types de données différents scénarios inspirés d'histoires réelles. Ces scénarios relatent un problème lié à la protection des données ou à la transparence dans le but de sensibiliser l'utilisateur de l'outil. Des conseils sont associés aux scénarios pour permettre aux utilisateurs de se positionner et d'améliorer le traitement des données au sein de leurs organisations.

Une première version de cet outil a été mise en ligne à l'occasion de la 6e journée de protection des données qui a eu lieu le 27 janvier 2012 (www.thinkdata.ch).

1.2 Protection des données – Questions d'ordre général

1.2.1 Protection des données et dons en cas de deuil

Les faire-part de décès invitent souvent à faire un don au profit d'une institution de bienfaisance au lieu de remettre des fleurs. Si ces institutions transmettent ensuite les informations concernant les dons reçus à la famille du défunt ou de la défunte, ceci peut constituer une divulgation de données personnelles. Nous expliquons donc dans quelles conditions une telle transmission de données est admissible du point de vue de la protection des données.

Lorsqu´un faire-part de décès contient une invitation à faire un don au bénéfice d´une institution de bienfaisance, les familles en deuil ressentent souvent le besoin de connaître les donateurs ainsi que les montants des dons, afin de pouvoir les remercier. À la suite de plusieurs demandes qui nous sont parvenues, nous avons constaté que ces organisations ne savent souvent pas quelles informations elles sont en droit de transmettre dans de tels cas.

Lorsqu´une institution de bienfaisance communique les noms des donateurs (ou toute autre information qui permet de les identifier), il s´agit d´une communication de données personnelles. Cela signifie que celle-ci doit respecter les conditions générales de la législation en matière de protection des données et que ces informations ne peuvent être communiquées à la famille endeuillée qu´avec le consentement du donateur. Comme il ne s´agit pas de données personnelles sensibles, une option de retrait (opt-out) suffit. Une manière de mettre ceci en œuvre consiste à prévoir un champ sur le bulletin de versement, dans lequel le donateur peut indiquer qu´il ne désire pas que ses données soient communiquées. Pour les personnes qui choisissent cette option, on se bornera à communiquer uniquement les données qui ne sont pas personnelles (tel que le montant du don).

Si la famille en deuil désire que ces donateurs reçoivent également une lettre de remerciement, ils peuvent la remettre à l´institution de bienfaisance. Celle-ci pourra transmettre ces lettres aux donateurs sans devoir dévoiler leur identité à la famille endeuillée.

1.2.2 Protection des données dans les bibliothèques

Il s'avère que les données des usagers de bibliothèques ne sont pas aussi anodines qu'elles pourraient paraître à première vue car, une fois combinées, elles peuvent former un profil de la personnalité significatif. C'est pourquoi nous avons publié un document expliquant comment traiter ce genre de données d'une manière qui soit conforme à la protection des données.

Une information en provenance des États-Unis a alarmé il y a quelques années le monde bibliothécaire: dans le cadre de sa lutte contre le terrorisme, le FBI (Federal Bureau of Investigation) a demandé à des bibliothèques américaines de leur remettre les données de leurs usagers. C´est au plus tard à ce moment-là qu´il est devenu évident que les informations apparemment anodines concernant les livres empruntés à la bibliothèque et les recherches effectuées dans ses ordinateurs pouvaient être reliées entre elles pour créer des profils de personnalité significatifs. Par conséquent, un examen du traitement des données personnelles dans les bibliothèques s´imposait afin de pouvoir, le cas échéant, l´adapter aux exigences de la protection des données.

Une invitation à un colloque de l´Association des bibliothèques juridiques suisses nous a incités à analyser les divers traitements de données effectués dans les bibliothèques et à rédiger une prise de position sur un traitement de ces données qui soit conforme aux exigences de la protection des données. Cette prise de position devrait notamment montrer comment les bibliothèques peuvent traiter les données personnelles dont elles ont besoin pour fournir leurs prestations, sans pour autant cumuler inutilement des informations qui pourraient être mises en relation pour créer ces fameux profils de la personnalité particulièrement délicats. L´accent est mis sur les données de base et de transaction des opérations de prêt ainsi que sur les traces laissées sur les ordinateurs avec accès Internet à disposition du public.

Les données de base doivent se limiter aux informations nécessaires pour le prêt et être supprimées une fois que la relation avec le client a pris fin ou au plus tard à l´échéance du délai légal de conservation. Les données concernant le prêt doivent être supprimées une fois qu´une opération de prêt a été bouclée. Dans les systèmes interconnectés, chaque bibliothèque doit avoir accès uniquement aux données des utilisateurs qui ont effectivement emprunté des livres dans cette bibliothèque.

Si la bibliothèque met à disposition de ses clients des ordinateurs avec accès à Internet, elle doit d'une part configurer le système de manière que les données de l´utilisateur soient automatiquement supprimées en fin de session et qu´un utilisateur ne puisse pas voir les données de la personne qui a utilisé l´ordinateur avant lui. D´autre part, nous recommandons que les ordinateurs ne puissent pas être utilisés de manière

anonyme. Nous jugeons opportun que les utilisateurs doivent, pour leur propre sécurité, s´enregistrer au préalable et que leurs données soient conservées pour une durée de six mois.

Plus d´informations sur la manière de traiter les données personnelles d´une bibliothèque en conformité avec la protection des données se trouvent dans l´article précité (www.leprepose.ch, sous Documentation – Protection des données – Articles, conférences, expertises sous «Autres contributions», uniquement sur le site version allemande) ainsi que sur notre site web www.leprepose.ch, sous Thèmes – Protection des données – Autres thèmes.

1.2.3 Exonération de la redevance radio et télévision

Au 1er janvier 2011, Billag SA a introduit de pair avec les assurances sociales un procédé conforme à la protection des données, exonérant les bénéficiaires de prestations complémentaires du paiement de la redevance radio et télévision. Dorénavant, il suffit pour les personnes concernées de fournir une attestation de leur assurance sociale.

Dans notre 17e rapport d'activités 2009/2010, ch. 1.2.9, nous avions déjà précisé qu'il était disproportionné de demander une décision définitive sur le droit à des prestations complémentaires, et le montant de celles-ci pour pouvoir bénéficier de l'exonération de la redevance. L'entreprise Billag SA a donc élaboré avec les assurances sociales une attestation standard. Ce document ne mentionne que la perception de prestations complémentaires, sans en préciser le montant. Depuis le 1er janvier 2011, les assurances sociales établissent cette attestation à l'attention de la société Billag SA et la remettent aux bénéficiaires des prestations en question.

1.2.4 Vidéosurveillance dans les transports publics

En nous fondant sur la loi fédérale sur le transport des voyageurs, nous avons procédé à des contrôles de la vidéosurveillance auprès de cinq entreprises de transport. Indépendamment de cela, l'Office fédéral de la justice a soutenu qu'il nous incombait d'apprécier la licéité des vidéosurveillances dans la mesure où celles-ci concernent l'activité exercée dans le cadre d'une concession.

Le 1er janvier 2010 a vu l'entrée en vigueur de la loi fédérale sur le transport des voyageurs et de la version révisée de la loi sur les chemins de fer. Cela signifie que toutes les activités des entreprises de transports publics, qu'elles soient exercées dans le cadre de leur concession et donc autorisées ou qu'elles soient de droit privé, sont régies

par la loi fédérale sur la protection des données. Il nous incombe d'en assurer la surveillance. La vidéosurveillance est explicitement réglementée dans les deux lois ainsi que dans l'ordonnance sur la vidéosurveillance dans les transports publics (cf. notre 18e rapport d'activités 2010/2011, ch. 1.2.3). Suite à l'utilisation croissante de la vidéosurveillance dans les moyens de transport public, nous avons décidé d'effectuer des contrôles auprès de plusieurs entreprises de transport au bénéfice d'une concession.

Nous avons examiné la vidéosurveillance dans les véhicules (trains, trams, bus), dans les gares/stations et dans les infrastructures (bâtiments, dépôts). Nos cinq contrôles ont montré que les entreprises concernées mettent correctement en œuvre leur vidéosurveillance et prennent au sérieux les aspects liés à la protection des données: ainsi, elles utilisent toutes des pictogrammes pour signaler la vidéosurveillance et définissent clairement les responsabilités, accès, flux de données, durée de conservation et conditions régissant la remise des images. L'appréciation des enregistrements est effectuée par des personnes déterminées, dans une pièce séparée sur des ordinateurs sécurisés, et uniquement en cas d'incident ou de sinistre. Dans un tel cas, les images en question sont évaluées, enregistrées sur un support de données séparé (clé USB ou CD-ROM) puis remis aux autorités de poursuite pénale.

En revanche, aucune des sociétés contrôlées n'a élaboré de concept écrit pour le traitement des demandes d'accès. Il est vrai qu'à ce jour personne n'a encore déposé une telle demande de renseignements en rapport avec une vidéosurveillance. Par conséquent, les dépouillements d'images effectués jusqu'ici ont toujours concerné des incidents concrets ou des sinistres. Nous avons attiré l'attention des entreprises sur le fait qu'un tel concept ne devait pas être compliqué. La personne qui fait valoir son droit d'accès doit pouvoir justifier son identité et indiquer la date, l'heure et le lieu où elle se trouvait dans l'angle de prise de vue d'une caméra exploitée par l'entreprise (voir notre lettre-type sur notre site web www.leprepose.ch, sous Services – Protection des données – Lettres-type – Vidéosurveillance). Le dépouillement des images peut alors être effectué de la même manière que dans le cas d'un incident. Au cas où les images auraient déjà été effacées, la personne concernée doit en être informée avec mention des délais de conservation. Les enregistrements, qui selon les cas peuvent être séparés de quelques minutes, sont transmis à la personne concernée, sous forme d'images imprimées, sur un cédérom ou comme séquence de film. Il est important de veiller à ce que toute personne tierce apparaissant sur les images soit auparavant rendue méconnaissable ou supprimée. Dans le concept, l'entreprise peut mentionner ces différentes manières de communiquer et indiquer qu'elle décidera de cas en cas des modalités exactes.

Lors des cinq examens effectués, nous n'avons pas eu besoin d'émettre des recommandations, mais avons néanmoins fait des propositions d'amélioration aux diverses

entreprises dans les cas où nous le jugions nécessaire. Nous avons notamment demandé l'élaboration du concept mentionné ci-dessus pour le traitement des demandes d'accès en rapport avec la vidéosurveillance. Les autres propositions d'amélioration concernaient par exemple l'élaboration d'un règlement écrit sur la vidéosurveillance, une meilleure sécurisation d'une porte donnant accès au local des serveurs ainsi qu'une méthode plus sûre pour la génération des mots de passe. Les entreprises ont accepté ces suggestions.

Dans le contexte de la nouvelle législation, l'Association des commissaires suisses à la protection des données Privatim a soumis à l'Office fédéral de la justice (OFJ) plusieurs questions sur la délimitation de nos responsabilités par rapport aux leurs ainsi que sur le droit applicable. Ceci après que l'OFJ ait retenu, dans une expertise datée de décembre 2010, que la disposition de la loi sur les transports de voyageurs, qui attribue la compétence de réglementation et de supervision de la protection des données à la Confédération, était conforme à la Constitution. Dans sa réponse à Privatim, l'OFJ a souligné qu'il fallait apprécier de cas en cas ce qui fait partie des activités autorisées au bénéfice d'une concession. Dans la mesure où une vidéosurveillance effectuée dans un dépôt de trams ou à un arrêt de bus concernait de telles activités, la licéité de la mesure devait être jugée selon la loi fédérale sur la protection des données et la compétence de surveillance incombait donc au PFPDT. En revanche, les aspects de protection des données liés à la relation de travail sont en principe régis par les réglementations cantonales.

1.2.5 Échange de données concernant les resquilleurs

Suite à une plainte déposée auprès de l'Office fédéral des transports comme autorité de surveillance, nous avons examiné la question de savoir si la législation sur la protection des données permettait aux entreprises de transport d'échanger leurs données relatives aux passagers qui ont été attrapés sans titre de transport valable.

Dans le cadre d´une plainte déposée auprès de l´autorité de surveillance, l´Office fédéral des transports (OFT) nous a priés d´examiner plus à fond l´aspect juridique de la protection des données. La question était de savoir s´il est licite que les entreprises de transport CarPostal, CFF, Thurbo et VBZ échangent les données qu´elles ont collectées sur les resquilleurs. Nos examens ont révélé ce qui suit:

Les entreprises qui sont au bénéfice d´une concession selon la loi fédérale sur le transport de voyageurs sont tenus d´avoir des tarifs qui doivent être appliqués de manière

identique à chacun. Les voyageurs qui ne peuvent pas présenter de titre de transport valable doivent payer un supplément; ce dernier peut être augmenté en cas de récidive.

S´appuyant sur cette base juridique, la Communauté de transports publics du canton de Zurich (ZVV) a créé un pool de données. Ce pool est une base de données centralisée, commune à l´ensemble du réseau tarifaire. Il contient les données de resquilleurs collectées par les bureaux d´encaissement (CFF, VBZ, CarPostal, Thurbo) et permet à ces derniers de comparer les données enregistrées. Le but de ce pool de données est de pouvoir appliquer le même tarif dans l´ensemble du réseau et de garantir l´égalité de traitement entre les voyageurs. Il se fonde sur une directive concernant le traitement des données relatives aux personnes voyageant sans titre de transport valable («Richtlinie über den Datenschutz für die Erhebung von Gebühren sowie die Erfassung von Personendaten und deren Aufbewahrung und Verwendung im ZVV-Datenpool bei Fahren ohne gültigen Fahrausweis»). Le pool de données est limité à la région tarifaire du ZVV.

Dans le cas présent, aussi bien les CFF que les transports de la ville de Zurich VBZ avaient saisi les données concernant le plaignant dans le pool de données ZVV. Les CFF recueillent les données des personnes voyageant sans titre de transport valable et se chargent de l´encaissement, aussi bien dans leur propre intérêt que dans celui d'autres entreprises de transport du ZVV. Les CFF saisissent dans le pool de données ZVV uniquement les données collectées dans le cadre du mandat de contrôle qui leur a été confié par le ZVV. Ainsi, dans le cas présent, les CFF ont effectué le contrôle dans le RER de Zurich sur mandat du ZVV, puis transmis les données au pool. Indépendamment de cette opération, les transports de la ville de Zurich VBZ ont également, en leur qualité d´office d´encaissement, saisi les données de la même personne dans le pool de données ZVV. Les deux entreprises, SBB et VBZ, disposent d´un accès clairement défini à ce pool de données. Les données enregistrées sont supprimées deux ans après l´incident.

Il apparaît clairement que dans le cas présent les données ont été saisies dans le pool ZVV dans le but de faire appliquer le tarif de manière uniforme et conformément aux dispositions susmentionnées. Ainsi, aucune communication de données illicite au sens de la loi sur la protection des données n´a eu lieu.

1.2.6 Vidéosurveillance de l´espace public effectuée par des particuliers

Que faire si l'on constate souvent la présence de personnes suspectes devant sa propriété ou si le jardin devant sa maison est utilisé comme décharge? La solution apparemment la plus simple consiste à installer une caméra vidéo qui surveille la route devant le jardin. Ceci n'est cependant pas admissible, à quelques exceptions près. Nous avons publié des informations complémentaires à ce sujet dans notre feuillet thématique «Vidéosurveillance effectuée par des particuliers».

L´utilisation de la vidéosurveillance dans le domaine de la sécurité s´est depuis longtemps établie en Suisse. De plus en plus de personnes installent des caméras sur leurs propriétés pour se protéger contre les visiteurs indésirables et pour faciliter la recherche des auteurs en cas de vandalisme, de cambriolage ou d'autres délits. Ce faisant, on éprouve souvent le besoin de surveiller également l´espace public situé devant la propriété privée. Ceci porte cependant atteinte aux droits de la personnalité d´un grand nombre de personnes. Ainsi, nous avons reçu ces derniers temps de nombreuses demandes de personnes concernées qui ont été filmées par de telles caméras vidéo privées dans l´espace public. Ces citoyens et citoyennes se sentent gênés par ces caméras, entravés dans leur liberté de mouvement et demandent à juste titre si une telle surveillance est permise.

Assurer la sécurité et l´ordre dans l´espace public est une tâche qui incombe en principe à la police. Si un problème de sécurité apparaît sur une propriété et qu´il provient de l´espace public, la première mesure à prendre est d´alerter la police. En règle générale, il n´y a donc pas de motifs justifiant l´installation d´un système privé de vidéosurveillance dans l´espace public. Plus de détails sur ce thème ainsi que sur les exceptions possibles se trouvent dans notre feuillet thématique «Vidéosurveillance effectuée par des particuliers» sur le site www.leprepose.ch sous Thèmes – Protection des données – Vidéosurveillance.

1.2.7 Enregistrement de données biométriques: variantes conformes aux exigences de la protection des données

Après le jugement rendu en la cause KSS, qui a qualifié d'atteinte disproportionnée à la personnalité des clients le stockage centralisé de données biométriques dans les établissements de loisirs, la question se pose de savoir comment stocker les données biométriques tout en se conformant aux exigences de la protection des données. Nous avons testé différentes variantes de stockage de ces données quant à leur conformité avec la protection des données et publié les résultats sur notre site web. Ces variantes devraient d'une part répondre aux besoins divers des exploitants de système, d'autre part sauvegarder les droits de la personnalité des personnes concernées.

Les données biométriques sont des données personnelles très particulières. Elles permettent d´identifier une personne sur la base de caractéristiques dépendantes de leur corps, qui ne peuvent ni être choisies librement, ni échangées ou modifiées facilement. Par conséquent, toute utilisation abusive de caractéristiques biométriques représente un très grave danger pour la personnalité des personnes concernées. C´est la raison pour laquelle les traitements de telles données doivent se conformer à des exigences sévères en ce qui concerne la protection et la sécurité des données. Ceci a également été reconnu par le Tribunal administratif fédéral qui a jugé un simple stockage centralisé de données biométriques dans le secteur des loisirs comme étant disproportionné.

Les systèmes de reconnaissance biométrique se répandent de plus en plus, aussi dans les établissements de loisirs. L'arrêt du Tribunal administratif fédéral soulève donc la question de savoir comment ces données peuvent être stockées sans violer les droits de la personnalité des personnes concernées. Nous avons examiné plusieurs variantes, en accordant une attention particulière aux divers besoins des exploitants de systèmes, notamment à la facilité de mise en œuvre dans la pratique. Nous sommes arrivés à la conclusion que pour pouvoir tenir compte du risque particulièrement élevé d´atteinte à la personnalité, les exigences suivantes doivent toujours et impérativement être remplies lors de l´utilisation d´un système de reconnaissance biométrique:

- Ces systèmes ne peuvent être utilisés que si les personnes concernées ont donné leur consentement. En d'autres termes, toutes les personnes concernées doivent être informées de manière adéquate sur le système. Elles doivent en outre pouvoir choisir une alternative qui n'utilise pas de caractéristiques biométriques.
- Les données biométriques brutes contiennent plus d´informations sur chaque personne qu´un gabarit (template) et peuvent éventuellement permettre de

tirer des conclusions sur l´état de santé ou la race d´une personne. Étant donné que les systèmes de reconnaissance biométrique ne requièrent pas une telle quantité d´informations, on utilisera des gabarits au lieu de données brutes.

- Afin de minimiser tout risque d´utilisation non autorisée, les gabarits doivent en outre être stockés sous forme chiffrée.

Pour la conception future d´un système de reconnaissance biométrique dans les établissements de loisirs, nous voyons trois possibilités:

- Les données biométriques sont stockées de manière décentralisée sur un support de données qui est en possession du client concerné. Cela garantit que cette personne garde le contrôle sur ses données biométriques et que ces données ne peuvent donc pas être utilisées sans une coopération consciente de sa part. Cette variante répond le mieux aux exigences de la protection des données et c'est donc celle-ci qu'il faut préférer.
- Les données biométriques sont stockées de manière centralisée. Elles ne peuvent cependant être rattachées à d'autres données personnelles que moyennant un code d'attribution qui est enregistré sur une carte détenue par la personne concernée. Ainsi, les données biométriques sortent de leur domaine de contrôle mais, comme les références à d'autres données de la personne concernée ne peuvent pas être établies sans sa collaboration consciente, le risque d'abus s'en trouve fortement limité.
- Les données biométriques sont stockées de manière centralisée. La référence à d'autres données personnelles n'existe pas et ne peut pas non plus être établie ultérieurement. Dans ce cas, seules des caractéristiques biométriques qui ne laissent pas de traces peuvent être utilisées (p. ex. forme des doigts, réseau veineux du doigt, forme de la main, mais pas les empreintes digitales, voir à ce sujet notre guide mentionné ci-dessous). Comme il n'y a pas de référence à d'autres données personnelles, le potentiel d'abus est fortement restreint. De plus, l'utilisation de caractéristiques biométriques ne laissant pas de traces garantit que les caractéristiques biométriques ne peuvent pas être recueillies et utilisées à l'insu des personnes concernées.

Plus de détails figurent dans notre complément au «Guide relatif aux systèmes de reconnaissance biométrique» sur notre site www.leprepose.ch, sous Documentation – Protection des données – Brochures.

1.2.8 Système de reconnaissance biométrique pour la réservation d´espaces sportifs: Clôture de la procédure

Un club de tennis a introduit un nouveau système de réservation avec reconnaissance biométrique des personnes. Notre examen sur place a montré que le système doit être adapté pour qu'il soit conforme aux exigences de la protection des données. Le club de tennis a accepté notre recommandation et met actuellement en œuvre les changements nécessaires.

Nous avions déjà constaté l´an dernier, lors de notre contrôle du système de réservation, que celui-ci ne satisfaisait pas aux exigences de protection des données à certains égards (cf. notre 18e rapport d'activités 2010/2011, ch. 1.2.6 et 4.1.2). Ainsi, les membres du club n'étaient pas suffisamment informés sur le traitement des données liées à la reconnaissance biométrique, le système était librement accessible sur le site web du club, aucun délai de destruction n'avait été défini, ni pour les données des membres, ni pour les données biométriques, et les moyens mis en œuvre pour assurer la sécurité physique et logique des données n'étaient pas suffisants. En particulier, les données dactyloscopiques étaient également stockées de manière centralisée sans mesures de sécurité supplémentaires, ce qui, selon l'arrêt du Tribunal administratif fédéral en la cause KSS, est absolument disproportionné.

Le club de tennis partage notre avis que la manière dont il a traité les données biométriques jusqu'ici n'est pas conforme aux exigences de la protection des données. Il a cependant déclaré que cela s'était fait sans mauvaises intentions et qu'il souhaitait protéger les droits de la personnalité de ses membres, et a entièrement accepté nos recommandations. L'information aux membres a été nettement améliorée, le site web remanié de manière à respecter les exigences de la protection des données, des délais de destruction des données ont été définis et diverses mesures ont été prises pour améliorer la sécurité des données. Au début du prochain exercice du club, le système de réservation actuel sera d'ailleurs modifié dans le sens que les données biométriques seront dorénavant enregistrées sur une carte individuelle en possession du membre concerné (cf. le complément au Guide relatif aux systèmes de reconnaissance biométrique sur notre site web www.leprepose.ch, sous Documentation – Protection des données – Brochures). Cela signifie qu'à partir de la mise en œuvre du nouveau système, aucune donnée biométrique ne sera plus stockée de manière centralisée et que les membres auront ainsi à nouveau le contrôle sur leurs données biométriques.

Avec ces adaptations, le club de tennis remplit nos exigences envers une utilisation proportionnelle et donc respectueuse de la protection des données de systèmes de reconnaissance biométrique. La procédure peut donc être close avec succès.

1.2.9 Stockage centralisé de photos de clients dans les stations de ski

Dans le cadre de l'établissement des faits effectué dans une station de ski, nous avons examiné le système de contrôle d'accès d'un fabricant renommé. Cet examen a révélé que le système satisfait en majeure partie aux exigences de protection des données mais que des améliorations sont nécessaires en ce qui concerne la sécurité des données lors du stockage central des photos des clients.

Un grand nombre de stations de ski en Suisse utilisent des systèmes de contrôle d´accès du même fabricant. Dans le cadre d'un examen effectué dans une station de ski suisse, des questions concernant la conformité de leur système avec la protection des données sont apparues. Nous avons alors pris contact avec le fabricant pour, avec sa collaboration, analyser ses produits et ainsi pouvoir mettre en œuvre les éventuelles améliorations de manière centralisée chez lui. Nous avons alors constaté que le système respecte la plupart des principes de protection des données pour autant que les stations de ski le configurent correctement. Ainsi, il est possible de configurer le système de manière qu´il collecte uniquement les informations nécessaires des clients, que celles-ci ne soient pas stockées plus longtemps que nécessaire et que les droits d´accès à certaines catégories de données soient définis de manière restrictive. D´autre part, le système a un concept clair et permet facilement de corriger ou de supprimer des données incorrectes. Il est donc possible d´exploiter le système de manière que le traitement des données soit proportionné et que l´exactitude des données puisse être garantie. Que ces systèmes soient exploités de manière conforme à la protection des données ou non dépend donc des stations de ski.

Le seul point d´amélioration que nous avons constaté concerne la protection des prises de vue, qui nécessite d´être adaptée. Le système a pourtant été conçu de sorte que les données ne puissent pas facilement être lues et utilisées à d´autres fins ou même soustraites. Mais, la base de données photographiques pouvant également contenir des données personnelles sensibles, cette protection doit être améliorée. Nous examinons actuellement avec le fabricant quelles mesures pourraient être mises en œuvre dans les futurs systèmes pour répondre entièrement aux exigences de protection des données.

1.2.10 Le traitement de données personnelles en relation avec des manifestations sportives

Dans le cadre de rencontres dites de sport de masse, les données personnelles de participants font l'objet de différents traitements. Nous avons donc soumis un fournisseur de services de la branche à un examen des faits. À cette occasion, nous avons pris en considération à la fois les traitements de données auxquels il procède lui-même et l'interface utilisateur qu'il offre aux organisateurs des événements sportifs.

D'une manière générale, les organisateurs d'un événement sportif qui désirent traiter des données personnelles doivent avoir un motif justificatif. Pour les participants, il est évident lorsqu'ils s'inscrivent que leurs données seront traitées dans le cadre de l'événement sportif afin d'établir la liste de départ, adresser des informations, attribuer un numéro de dossard, établir les listes de classement à afficher, ainsi que pour la cérémonie de remise des prix, les comptes-rendus dans les médias et les informations des commentateurs. Ces utilisations sont justifiées par l'intérêt privé des organisateurs et l'intérêt public rattaché à la manifestation sportive.

Néanmoins, une communication de données par l'organisateur sur Internet, par exemple sous forme de publication des listes de départ, de listes de classement ou sous forme de lien avec des photos de l'événement sportif ne va généralement pas de soi. C'est la raison pour laquelle ce genre de communication doit être indiqué dans la déclaration de protection des données ou figurer dans la description des prestations contenues dans les frais d'inscription. La personne concernée doit avoir la possibilité de contester une telle publication de ses données sur Internet.

De même, l'organisateur n'est pas autorisé à transmettre sans information préalable des données personnelles à des tiers, par exemple à des photographes qui, après la manifestation, vendent des photos à des participants ou à des entreprises qui poursuivent des objectifs publicitaires. Toutefois, il ne suffit pas d'insérer un renvoi dans le règlement ou dans la déclaration de protection des données; en effet, ce genre de traitement de données est inhabituel en marge des manifestations sportives. L'organisateur doit donc disposer du consentement valable des participants; ce consentement présuppose que l'on a attiré explicitement leur attention sur la transmission de données se rapportant à des personnes, sur son but ainsi que sur les possibilités de s'opposer à la publication.

Nous demandons donc aux organisateurs de manifestations sportives de présenter clairement et de manière complète sur le formulaire d'inscription ou sur l'inscription en ligne les finalités du traitement de données et de préciser à quels tiers les données seront communiquées. En outre, les organisateurs doivent donner la possibilité à tout

participant de refuser que ses données personnelles soient publiées (sur Internet, dans des journaux) ou transmises à des tiers. Nous suggérons de prévoir à cet effet une case à cocher sur le formulaire ou par l'indication d'une possibilité de contact (e-mail, téléphone ou autres) auprès de laquelle le participant peut faire valoir son refus.

L'interface d'administration offerte aux organisateurs favorise un traitement proportionné des données. Ainsi le fournisseur a limité les données personnelles saisies dans le système à celles qui sont nécessaires à l'organisation. L'effacement, à la fin de la manifestation, des numéros de téléphones librement indiqués pour pouvoir envoyer les SMS nécessaires au déroulement de l'événement sportif, fait également partie de ce traitement proportionné des données. Pour ce qui est des banques de données, une solution est offerte aux organisateurs permettant de séparer clairement ces banques de données et de traiter les informations requises. En outre, la création de listes à partir des informations nécessaires à la manifestation sportive est limitée. Pour ce qui est des données personnelles appartenant aux organisateurs, le mode d'accès et d'effacement doit encore être adapté au cas où les demandes sont adressées par erreur aux fournisseurs.

1.2.11 Publication de photos de hooligans par un club de football

Un club de football n'a pas le droit de publier sur son site web des photos de personnes soupçonnées d'avoir lancé des pétards et pas non plus d'appeler les visiteurs du site à communiquer toute information utile sur les personnes en question. Un tel avis de recherche public est exclusivement du ressort de la police, dans les cas où les conditions requises sont remplies.

Un club de football a publié sur son site les photos de deux personnes en exhortant les visiteurs à communiquer par courriel toute information utile concernant les deux hommes (dont l´un était présumé avoir lancé des pétards et l´autre l´y avoir aidé). Les hommes ont rapidement pu être identifiés, sur quoi les images ont été retirées du site.

Nous avons attiré l´attention du club sur le fait qu´il n´avait pas le droit de publier des photos de cette façon. À notre avis, une telle publication ne peut pas être justifiée au sens de la loi sur la protection des données, étant donné que ni l'assentiment de la personne concernée, ni un intérêt prépondérant public ou privé, ni une loi n´existe. La démarche correcte consisterait à remettre les photos, accompagnées d´une plainte pénale, à la police. Il incomberait ensuite à celle-ci de vérifier si les conditions permettant une publication sur son site web sont réunies, comme l´a fait par exemple la police municipale de Zurich avec un avis de recherche public.

1.2.12 Formulaire pour le contrôle médical subséquent effectué par un médecin-conseil

Le contrôle médical subséquent effectué par un médecin-conseil en vue de vérifier l'aptitude à conduire ainsi que les formulaires correspondants font l'objet d'une réglementation au niveau fédéral. L'appréciation du traitement des données effectué par le service cantonal des automobiles relève cependant de la compétence de l'autorité cantonale de protection des données.

Nous avons reçu diverses demandes en rapport avec ces contrôles médicaux. Ces contrôles sont réglementés au niveau fédéral, à savoir dans l´ordonnance réglant l'admission des personnes et des véhicules à la circulation routière (OAC). L´article 27 de cette ordonnance précise qui doit se soumettre à un tel examen médical. Sont concernés en particulier tous les conducteurs âgés de plus de 70 ans. La formule reproduite à l´annexe 2 de l´OAC énumère les points qui sont examinés lors de ce contrôle médical. En revanche, le résultat de l´autorité cantonale doit être communiqué par la formule de l´annexe 3 (art. 27 OAC, ch. 3). La responsabilité d´apprécier si le service cantonal des automobiles traite correctement ces données incombe à l´autorité cantonale de protection des données.

1.2.13 Contrôles relatifs à l'élaboration des règlements de traitement dans l'administration fédérale

Dans le cadre de notre activité de surveillance, nous avons vérifié auprès de plus d'une vingtaine d'offices s'ils respectaient leur obligation légale d'élaborer un règlement de traitement pour les fichiers répondant à certains critères. Ce contrôle a mis en lumière d'importantes lacunes et nous a permis d'attirer l'attention des conseillers à la protection des données des offices fédéraux concernés sur leurs obligations légales et sur nos explications relatives à l'élaboration d'un tel règlement de traitement.

Au cours de l'année sous revue, nous avons vérifié auprès de plus d'une vingtaine d'offices s'ils respectaient leur obligation légale d'élaborer un règlement de traitement pour les fichiers répondant aux critères de l'article 21, 1er alinéa, de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD). Ce dernier stipule que les organes fédéraux sont tenus d'établir un règlement de traitement pour les fichiers automatisés, notamment s'ils contiennent des données personnelles sensibles ou des profils de la personnalité ou s'ils sont utilisés par plusieurs organes fédéraux.

L'objectif de ce contrôle était de vérifier l'existence des règlements de traitement et non pas de nous prononcer sur le contenu de ces derniers. Nous avons contrôlé une trentaine de fichiers et avons constaté de manière générale que l'obligation d'élaborer un règlement de traitement était souvent méconnue. Ainsi, plusieurs règlements de traitement faisaient défaut ou avaient été rédigés il y a plusieurs années sans être mis à jour depuis. D'autres fichiers étaient annoncés dans notre registre alors qu'ils n'existaient plus. Nous avons donc profité de ce contrôle afin de rappeler aux conseillers à la protection des données des offices fédéraux concernés leurs obligations légales et nous avons attiré leur attention sur nos explications relatives à l'élaboration d'un règlement de traitement publiées sur notre site web www.leprepose.ch, sous Documentation – Protection des données –Brochures – Mesures techniques et organisationnelles. Nous leur avons par ailleurs rappelé qu'indépendamment de l'obligation légale précitée, toute mise en place d'un système d'information dans l'administration fédérale implique l'élaboration d'un règlement de traitement déjà au niveau de la phase d'analyse préliminaire de tout projet informatique, comme le prévoit clairement la procédure Hermes (cf. point 3.3.4 du manuel Hermes: Adaptation de systèmes, respectivement point 3.3.3: Développement de systèmes).

Ce contrôle a permis une importante sensibilisation aux lacunes constatées dès lors qu'au début de notre contrôle, seuls 10 fichiers parmi les 34 contrôlés possédaient un règlement de traitement, alors qu'au terme de notre contrôle tous les fichiers répondant aux critères de l'article 21 OLPD sont dotés d'un règlement de traitement.

1.2.14 Exigences envers un règlement de traitement

Le règlement de traitement s'élabore déjà dans les étapes de planification d'un projet pour être ensuite mis à jour dans la phase d'exploitation du système. Afin d'effectuer cette mise à jour, la personne responsable doit disposer des informations nécessaires, notamment sur les modifications apportées au système et sur les contrôles effectués.

Le règlement de traitement est destiné à assurer la transparence nécessaire aussi bien en termes de protection des données que de sécurité des données et de l´information. La première version du règlement de traitement doit être disponible au terme des phases de planification du projet. Il est ensuite mis à jour durant la période d´exploitation du système. En phase d´exploitation, il s´agit de documenter en particulier tant les modifications apportées au système que les contrôles effectués avec leurs résultats. Il convient de noter qu´une telle documentation ne peut être mise à jour que si la personne qui a élaboré le règlement et le complète par la suite obtient les informations nécessaires.

Nos exigences envers un règlement de traitement sur notre site web www.leprepose.ch, sous la rubrique Documentation – Protection des données – Brochures – Mesures techniques et organisationnelles, dans la colonne de droite. Hermes, le standard de l´administration fédérale suisse pour la gestion et l´exécution des projets relatifs aux technologies de l´information et de la communication, attire l´attention à plusieurs reprises au stade de l´analyse préliminaire sur le règlement de traitement de la protection des données. Le règlement de traitement constitue un résumé clair des points importants en matière de protection des données et de sécurité de l´information. Au cas où des informations (telles qu´un concept de sécurité ou une documentation détaillée des processus) ont été élaborées de manière plus approfondie, le règlement y renverra, après une documentation de synthèse dans le règlement même. Le règlement de traitement doit être rédigé de manière claire et concise, de manière que même des non-spécialistes puissent comprendre et juger le système.

1.3 Internet et télécommunication

1.3.1 Géolocalisation à l'aide d'appareils mobiles

Les appareils mobiles permettent de relever des données de position géographique pour des services de géolocalisation. Si ces données sont stockées sur une longue période, elles permettent d'établir un profil de mouvement détaillé des utilisateurs des appareils. Dans le cadre d'un examen des faits, nous avons donc analysé les traitements de données qu'Apple réalise à ce sujet; en même temps Apple lançait une mise à jour du logiciel permettant d'empêcher la saisie des données de position géographique.

Au printemps 2011, on a appris que les appareils mobiles fonctionnant sous iOS enregistraient des données de position géographique, les envoyaient à Apple et en plus, les déposaient sur les ordinateurs chargés de les synchroniser. Étant donné que la collecte de données de positionnement relatives à une personne ou un appareil constitue un traitement de données personnelles, nous avons procédé à un examen des faits.

Selon Apple, tous les emplacements d'antennes de téléphonie mobile et de bornes Wi-Fi (hotspots) n'étaient pas enregistrés par l'appareil lui-même. La société Apple fournissait elle-même des informations relatives à des emplacements se trouvant éventuellement à proximité du téléphone. L'objectif de cette collecte de données est de permettre de déterminer plus rapidement la position de l'appareil pour diverses applications.

En outre, en raison d'une erreur de programmation, les emplacements d'antennes étaient saisis dans le secteur de réception de l'appareil même après la désactivation des services de localisation et étaient envoyés à Apple. La mise à jour iOS du 4 mai 2011 a permis d'éliminer cette erreur. Par ailleurs, depuis la mise à jour, le fichier avec les données de position géographique n'est plus sauvegardé par l'intermédiaire du programme iTunes sur d'autres appareils. Les données collectives recueillies par les utilisateurs («crowd-sourcing») en matière de Wi-Fi, hotspot et téléphonie mobile sont effacées au bout de sept jours et toutes les informations de localisation temporaires sont effacées lorsque les services de localisation sont éteints.

Les modifications générées par la mise à jour mentionnée du système d'exploitation permettent aux utilisateurs d'effacer les informations locales ainsi que d'empêcher leur saisie et leur transmission. Les exigences posées par le droit de la protection des données étaient ainsi satisfaites et nous avons pu clore notre examen des faits.

Il reste toutefois à souligner qu'indépendamment du système d'exploitation, les utilisateurs sont, comme auparavant, libres de choisir les applications, programmes ou

fabricants auxquels ils confieront leurs données (de positionnement) et livreront éventuellement des informations permettant d'établir un profil (de mouvement) détaillé. Dans le but de réduire au maximum les risques liés à ces actions, ils devraient d'une part lire attentivement les conditions générales de vente et la déclaration de protection des données de la marque, d'autre part adapter les paramétrages d'accès pour les programmes.

1.3.2 Marketing en ligne: protection des utilisateurs d'Internet

En novembre 2009, le parlement de l'UE a révisé la Directive «Vie privée et communications électroniques». Une des modifications importantes concerne les exigences relatives au stockage des cookies sur un terminal, ou à l'accès à ces derniers. La solution de l'option de retrait (opt-out) proposée dans l'ancienne version de la directive a été remplacée par une solution de «consentement informé» (informed consent), c'est-à-dire par une volonté (opt-in) exprimée par l'utilisateur après avoir été informé en détail sur la nature et le but du traitement des données.

Il est faux de croire que l´on est anonyme lorsqu´on navigue sur le web. L´Internet est un média interactif, et chaque visite d´un site web laisse des traces sous forme d´informations collectées. Ainsi, la méthode de l´«online tracking», qui enregistre les actions des utilisateurs sur plusieurs sites web, utilise divers procédés et moyens en fonction des buts poursuivis. Elle constitue une atteinte à la vie privée et peut, dans une certaine mesure être contournée par des mesures techniques, ce qui est rarement le cas étant donné que les utilisateurs ne s´en rendent pas compte.

Les nouvelles exigences de l´UE ont créé passablement de remous, notamment dans le secteur du marketing en ligne. Cette branche réalise une grande partie de ses revenus publicitaires grâce à ce ciblage comportemental («Online Behavioral Advertising» – OBA). On regroupe sous cette appellation toutes les offres publicitaires qui s´affichent sur l´écran de l´utilisateur en se basant sur les données collectées lors des visites précédentes, le plus souvent à l´aide de cookies. Inquiétés par les nouvelles dispositions de l´UE, nombre d´acteurs importants y ont vu une mise en danger de la publicité en ligne allié à une crainte que les prestations gratuites sur Internet puissent disparaître.

La «European Advertising Standards Alliance» ainsi que le «Interactive Advertising Bureau Europe» désirent empêcher une législation stricte dans les États membres de l´UE et ont donc élaboré un code de conduite («Code of Conduct») comme mesure d´autorégulation pour leurs membres. Ce code prévoit, pour l´essentiel, une option de retrait (opt-out) qui permet à l´utilisateur de s´opposer à l´enregistrement de

ses habitudes de navigation. Le Groupe de travail «Article 29» – l´organe consultatif de la Commission européenne en matière de protection des données –, a cependant relevé une nouvelle fois dans un document publié en décembre 2011 que les mesures d´autorégulation proposées ne satisfaisaient pas aux exigences légales. Selon lui, l´information et la transparence lors de l´utilisation des outils OBA doivent être améliorées. Il est en outre d´avis que le système «opt-out» proposé pour s´opposer à recevoir de la publicité en ligne ciblée est incompatible avec l´option «opt-in» prévue dans la directive pour les cookies.

Certains États membres de l´UE ont déjà mis en œuvre les exigences de la directive dans leur droit national, alors que d´autres ont encore du mal. En fait, il semble que cela représente un énorme défi de répondre aux exigences légales du «consentement informé», tout en évitant de limiter trop fortement la convivialité lors de la navigation sur Internet.

Alors que les pays européens s'occupent de la problématique des cookies, les États-Unis luttent pour trouver leur propre solution, qui devrait restreindre l´accès quasi illimité des entreprises aux données privées sur Internet. L´administration Obama a lancé un vaste projet de loi, qui – selon un rapport publié dans le «Wall Street Journal» – trouve l´appui des démocrates, mais aussi des milieux industriels, tels que Microsoft. Ils ne sont pas les seuls, puisque même les principaux organismes du commerce tels que la «Federal Trade Commission» (FTC) et la «Chamber of Commerce» sont devenus actifs: voyant d´un côté les préoccupations grandissantes des citoyens et de l´autre une activité de suivi quasi illimitée, de même qu´une vive commercialisation des données privées, les gouvernements se sentent obligés d´intervenir.

Les utilisateurs disposent eux aussi de moyens pour endiguer l´enregistrement par des tiers de leurs actions sur la Toile. Les principaux navigateurs web tels que Internet Explorer, Mozilla Firefox, Safari ou Google sont aujourd´hui équipés de fonctions de respect de la vie privée. Tout d´abord, il est conseillé d´installer toujours la dernière version d´un navigateur. Ensuite, il est possible de gérer les cookies à l´aide de fonctions de recherche et de réglages spécifiques. Une autre méthode permettant de limiter le suivi des visites de site consiste à utiliser le mode «navigation privée». Dans Chrome, la fonction s´appelle «Incognito». Il y a cependant lieu de noter que le mode «navigation privée» ne bloque pas les cookies. Par contre, une fois que l´on ferme le navigateur ils sont tous supprimés de même que l´historique des sites visités. L´installation de modules d´extension (Plugins ou Addons) dans le navigateur peut en outre contribuer à mieux contrôler les atteintes à la vie privée.

Nous soutenons d´une part les initiatives privées visant à améliorer le respect de la vie privée dans le domaine du marketing en ligne, en dialogue avec les représentants de la

branche en Suisse. D´autre part, nous suivons de près les développements à l´étranger. Bien sûr, une solution spéciale pour la Suisse est impensable, ne serait-ce que parce que les sites web des prestataires ou des réseaux publicitaires suisses ne s´arrêtent pas à nos frontières. Il est incontestable que l´information et la transparence doivent être garanties lors de l´utilisation de ces outils de traçage. En fonction de la sensibilité des données traitées, les exigences envers le devoir d´information peuvent être accrues. Il se peut même que certains traitements nécessitent le consentement explicite de l´utilisateur pour qu´ils soient autorisés.

1.3.3 Courriels non sollicités (pourriels ou spam)

Nous recevons régulièrement des demandes sur le thème des pourriels, par exemple sur la qualification d'adresses de courriel en tant que données personnelles. Par ailleurs, le cadre réglementaire a été adapté durant ces dernières années aux défis techniques. Ceci nous incite à exposer succinctement la situation de droit actuelle.

Par pourriel (ou spam) il faut entendre un message électronique non sollicité, généralement indésirable et répété, envoyé en masse. Nous avons abordé ce sujet à plusieurs reprises déjà (cf. notre 9e rapport d'activités 2001/2002, ch. 8.2, et notre 10e rapport d'activités 2002/2003, ch. 8.1 et 13.7.3). La Commission fédérale de la protection des données a confirmé notre avis par son arrêt du 15 avril 2005: les adresses de courriel sont des données personnelles au sens de la loi sur la protection des données – qu'il s'agisse ou non de désignations de fantaisie. Le but protecteur de la loi est en conséquence déterminant: Selon le jugement, lorsque des personnes mettent à disposition des canaux de communication actifs (numéros de téléphone, adresses de courriel) et sont atteignables de cette manière, il existe un couplage incontestable entre les personnes et ces données. La personne a droit à l'autodétermination individuelle en matière d'information dans le cadre que lui accorde la loi. C'est pourquoi – sous réserve de dispositions contraires – elle détermine seule si ses données peuvent être traitées ou non. Le fait que ces données soient constituées de séries de chiffres ou de désignations de fantaisie ne peut jouer aucun rôle, tant qu'elles sont explicitement attribuées à cette personne. C'est clair d'emblée pour les numéros de téléphone. Il n'en va pas autrement des adresses de courriel (Jugement de la Commission fédérale de la protection des données du 15 avril 2005, consid. 2.4).

Une collection d'adresses de courriel (telle que les expéditeurs de spams en constituent) est ainsi un fichier de données personnelles et la personne dont l'adresse de courriel y figure a, aux termes de la loi sur la protection des données, un droit d'accès envers le maître de fichier. La provenance des données doit être clairement révélée,

dans la mesure où les indications correspondantes sont disponibles pour le maître de fichier.

D'autres lois fédérales offrent également des moyens légaux pour agir en cas de harcèlement par des courriels non sollicités: Depuis le 1er avril 2007, la législation suisse interdit expressément l'envoi de courriels non sollicités. La loi fédérale contre la concurrence déloyale (LCD) prévoit plusieurs actions de protection face au pollupostage. La loi sur les télécommunications (LTC) prévoit les mesures que les fournisseurs de services de télécommunications sont tenus de prendre contre le spam.

Pour être licite, le publipostage de masse par Internet ou par voie de télécommunication doit remplir les conditions suivantes:

- Les messages publicitaires ne peuvent être envoyés qu'aux destinataires qui ont préalablement consenti à en recevoir (option d´adhésion ou «opt-in»). Les expéditeurs de publicité de masse doivent disposer du consentement exprès du destinataire avant même l'envoi du premier courriel.
- L´expéditeur de la publicité doit être clairement identifiable. Son adresse doit être indiquée correctement. L'identité de l'expéditeur ne doit être ni camouflée, ni falsifiée.
- Dans chacun de ses messages publicitaires, l'expéditeur doit offrir aux destinataires la possibilité de refuser facilement et gratuitement l'envoi d'autres messages et il doit les informer clairement de cette possibilité.

Les bases légales concernant le spam figurent en détail sur notre site web www.leprepose.ch, sous Documentation – Protection des données – FAQ – Informatique de même que des conseils pratiques pour éviter d´être importuné par des spams.

1.3.4 Prises de vue des voies publiques sur Internet

Dans notre 18e rapport d'activités 2010/2011, au ch. 1.3.3, nous avions informé sur l'arrêt du Tribunal administratif fédéral (TAF) dans l'affaire Google Street View; le TAF avait approuvé nos recommandations sur tous les points essentiels et leur avait donné un caractère obligatoire. Google a déposé un recours contre ce jugement devant le Tribunal fédéral. Le TAF a, comme nous d'ailleurs, pris position sur les allégués du recourant en demandant que le recours soit entièrement rejeté. Le jugement du Tribunal fédéral est attendu prochainement.

1.3.5 Intégration de plugins sociaux sur des sites Internet

L'intégration de contenus Internet de fournisseurs tiers n'est pas un nouveau phénomène. Si au début, il s'agissait d'informations boursières ou de bulletins météorologiques, on nous offre aujourd'hui, à l'ère du «tout interactif», la possibilité de commenter ou d'intégrer articles ou blogs. Afin de faciliter cette interactivité, les fournisseurs de réseaux sociaux offrent leurs plugins aux éditeurs de site Internet. Mais leur intégration n'est pas sans poser quelques problèmes du point de vue de la protection des données.

En 2006, nous nous sommes déjà exprimés sur une question analogue, celle des «webbugs» (les pixels espions), nous avons exposé les problèmes qui se posent au regard de la protection des données et indiqué quelles possibilités d'action s'offraient aux éditeurs de sites et aux utilisateurs d'Internet (voir www.leprepose.ch), Thèmes – Protection des données – Protection technique des données – Thèmes techniques). L'utilisation de plugins sociaux est aujourd'hui un thème comparable; leur forte diffusion accentue toutefois les problèmes de protection des données. Il convient de souligner à cet endroit les possibilités de traçage dont disposent les fournisseurs; en effet, l'information signalant qu'un site Internet contenant des plugins sociaux est visité est transmise dès que le site est appelé.

Afin de se conformer aux exigences de loi suisse sur la protection des données, l'éditeur d'un site Internet qui intègre les contenus de fournisseurs tiers doit tout particulièrement veiller à informer de manière précise les utilisateurs de son site Internet sur les traitements de données liés à la visite de ce site. Sont également disponibles sur notre site Internet des indications détaillées sur les points que doit comporter une déclaration de protection des données et comment procéder pour rédiger cette déclaration (voir www.leprepose.ch, FAQ – Protection des données – Commerce et économie – Déclarations de traitement des données dans le commerce électronique).

Par ailleurs, les éditeurs de sites Internet doivent prendre des mesures techniques et organisationnelles appropriées afin d'éviter les atteintes injustifiées aux droits de la personnalité. Dans le contexte concret des plugins sociaux, nous renvoyons aux possibilités de mise en œuvre conformes aux principes de protection des données, librement accessibles sur Internet (boutons de recommandation à deux clics).

Pour leur part, les utilisateurs d'Internet doivent assumer leur responsabilité en adaptant leur comportement en matière de navigation et la configuration de leurs logiciels en fonction des possibilités existant aujourd'hui sur Internet et en trouvant le juste milieu entre la protection de leur sphère privée et un confort d'utilisation qui réponde à leurs besoins.

1.3.6 Plateforme Internet d´évaluation des bailleurs immobiliers

Un site web permet aux locataires de faire part de leurs commentaires sur leurs bailleurs et de les évaluer. Les exploitants de cette plateforme d'information et d'évaluation espèrent ainsi améliorer la transparence sur le marché de la location immobilière. Du point de vue de la protection des données, ces plateformes peuvent toutefois entraîner des problèmes juridiques.

Un site web permet aux locataires de la Suisse entière de faire part, anonymement, des expériences qu´ils ont faites avec leurs bailleurs. Dans un premier temps, ils communiquent les données de leur bailleur. Ils procèdent ensuite à une évaluation en répondant à des questions standardisées. Les réponses aux questions sont données en attribuant de zéro à cinq étoiles. Le nombre d´étoiles recueillies est ensuite converti moyennant un système d´évaluation pour donner finalement un taux de recommandation.

En principe, de telles plateformes peuvent être utiles en tant que source d´information pour certains publics cible. Elles présentent cependant un gros risque d´atteinte à la personnalité. Sous l´angle de la protection des données, il importe tout d´abord de préciser que l´exploitant du site en question doit savoir qu´il répond lui-même de la publication de données personnelles sur son site. À ce jour, les bailleurs n´ont pas été informés que des données les concernant avaient été enregistrées et n´ont donc eu aucune possibilité de donner leur consentement, ni à la publication, ni à l´évaluation subséquente. Pourtant, une publication de données de bailleurs immobiliers sur un site web constitue un traitement de données personnelles selon la loi sur la protection des données, qui, de toute évidence, ne peut être justifié que par le consentement des personnes concernées. Nous avons fait remarquer aux exploitants de ce site qu´il est indispensable d´informer de manière détaillée les bailleurs sur le traitement des données personnelles et sur le but poursuivi et d´obtenir leur consentement.

D´autre part, il faut être conscient du fait que la publication sur le web d´informations concernant une entreprise ou une personne peut constituer une atteinte à la personnalité. Pour éviter cela, l´exploitant devrait donc prendre certaines précautions. Les locataires qui émettent des critiques anonymes devraient s´identifier sur le site, de manière que leur identité soit connue de l´exploitant du site et qu´ils puissent être poursuivis en cas d´atteinte grave à la personnalité. Cela n'était pas le cas sur le site susmentionné. Les visiteurs pouvaient s´y enregistrer simplement en indiquant leur adresse de courriel, puis déposer de manière anonyme leurs préoccupations, commentaires et évaluations.

Nous avons expliqué aux exploitants quelles étaient les lacunes de leur site en termes de protection des données et avons discuté avec eux des améliorations possibles. Les responsables ont pris connaissance de nos remarques et cherchent maintenant des moyens de remanier leur site pour combler ces lacunes. Le site web reste hors service jusqu´à la réalisation de ces modifications.

1.3.7 Échange de contenus sur Internet – Situation juridique après l´arrêt Logistep

L'arrêt Logistep du Tribunal fédéral a encore requis notre attention durant l'année sous revue. Nous avons notamment indiqué les conditions dans lesquelles, à notre avis, des particuliers peuvent, aussi après le jugement, traiter des données personnelles dans le cadre de la poursuite de violations du droit d'auteur sur Internet de manière conforme à la protection des données.

Dans notre 18e rapport d'activités 2010/2011, ch. 1.3.5, nous avons rendu compte de l'arrêt du Tribunal fédéral en la cause Logistep (ATF 136 II 508). Le tribunal avait exprimé dans ses considérants son malaise face à l'actuelle réglementation légale manifestement ressentie comme insuffisante. Dans son rapport de gestion 2010 (p. 17), il indiquait aussi explicitement qu'il appartenait au législateur de «prendre les mesures nécessaires pour assurer une protection des droits d'auteur appropriée aux nouvelles technologies.»

Nous sommes toutefois d'avis que les considérants faisaient aussi à Logistep, respectivement à son mandant, le reproche d'avoir en partie profité d'incertitudes créées par l'entreprise même pour faire valoir des prétentions civiles (excessives). Et ceci avant que la culpabilité de personnes présumées violer le droit d'auteur n'ait été constatée définitivement dans une procédure pénale satisfaisant aux exigences d'un État de droit.

Selon nos recherches en 2008, c´est précisément sur ce point que la démarche d´autres détenteurs de droits d´auteur poursuivant des personnes présumées avoir violé les droits d´auteur diffère de celle adoptée par Logistep: ainsi, l´IFPI Suisse (l´association faîtière des producteurs de supports sonores et audiovisuels) attend toujours une condamnation pénale exécutoire avant de se porter partie civile contre les personnes ayant violé les droits d´auteur. Nous avons informé l´IFPI Suisse en mars 2008 déjà qu´à notre avis elle ne viole pas la loi sur la protection des données avec cette manière de procéder.

Suite à la décision Logistep, l´IFPI Suisse et SAFE (Association suisse pour la lutte contre le piratage) ont pris contact avec nous. Les deux associations nous ont assuré que leur

démarche correspond à celle qui nous a été présentée au printemps 2008. Nous leur avons donc communiqué qu´il nous paraissait toujours possible d´admettre un intérêt prépondérant, justifiant donc les atteintes à la personnalité liées à ces traitements de données,

- s´il est assuré que la collecte et l´enregistrement des données ne va pas au-delà de ce qui est absolument nécessaire pour déposer (auprès des autorités locales compétentes) une plainte pénale contre des personnes présumées avoir violé les droits d´auteur;
- s´il est assuré que les négociations pour les prétentions en réparation du dommage menées entre les détenteurs des droits d´auteur et les personnes présumées avoir violé ces droits n´ont lieu qu´à leur initiative ou alors après une condamnation pénale exécutoire;
- et si les détenteurs des droits d´auteur intensifient leurs efforts afin de rendre la collecte des données personnelles et le but de leur traitement aussi reconnaissables que possible pour les personnes concernées. Ils doivent à cet effet, notamment à un emplacement aisément accessible et visible sur leurs sites web, révéler en toute transparence leur manière de procéder (y compris des indications détaillées sur la nature et l´étendue des données collectées) et exprimer clairement que des actions en réparation du dommage ne seront engagées qu´envers des personnes condamnées pénalement avec force exécutoire pour violation des droits d´auteur.

Nous avons attiré en outre l´attention de SAFE et de l´IFPI sur le fait que les fichiers devaient être enregistrés chez nous lorsque des données personnelles sensibles ou des profils de personnalité sont régulièrement communiqués à des tiers.

Dans ces conditions, il reste à notre avis toujours possible d´engager des poursuites conformes à la protection des données en cas de violation des droits d´auteur sur Internet. Toutefois, comme nous n´avons pas – de par la loi – le pouvoir d´approuver formellement des traitements de données, une évaluation juridiquement contraignante ne peut être faite que par les tribunaux compétents, comme dans le cas Logistep.

Dans ce contexte, il importe encore de relever que si les tribunaux pénaux devaient instaurer une jurisprudence stable selon laquelle les adresses IP collectées par des particuliers ne sont généralement pas utilisables dans une procédure pénale, nous devrions revoir notre analyse. Du point de vue de la protection des données, l´enregistrement et la communication des adresses IP par des particuliers ne seraient plus possibles selon le droit applicable lors d´actions intentées pour violation des droits d´auteur. La collecte de données serait d´emblée inappropriée pour le but poursuivi, et le traitement des données disproportionné en conséquence.

1.3.8 Surveillance électronique: protection contre la copie des jeux informatiques

Un jeu pour ordinateur sorti l'automne dernier a causé un certain émoi dans la presse. Apparemment, le système de protection contre la copie de ce jeu espionnait les ordinateurs des utilisateurs et transmettait au fabricant des informations sur les données stockées sur l'ordinateur, sur le comportement des utilisateurs et bien plus encore. Nous sommes actuellement en train d'analyser le logiciel contesté quant à sa conformité avec la protection des données.

Tout utilisateur qui désire utiliser le jeu en question doit d´abord installer une application supplémentaire et s´enregistrer auprès du fabricant sur une plateforme web. Le but de cette mesure est apparemment d´empêcher l´utilisation de copies piratées. L´installation de l´application et l´enregistrement sont obligatoires, indépendamment du fait que l´on joue en mode multijoueur en ligne ou seulement en mode monojoueur hors connexion. Après la sortie du jeu, les médias ont largement rapporté que les joueurs étaient espionnés à l´aide de cette application. Selon eux, le fabricant recevrait des informations détaillées concernant toutes les activités de l´ordinateur en question ainsi que sur tous les fichiers qui y sont stockés sans que l´utilisateur ne remarque quoi que ce soit. D´autres informations de presse ont plus tard relativisé en partie cette représentation.

Nous avons entretemps été contactés par de nombreux joueurs inquiets. Ceci nous a incités à contacter le siège suisse de ce fabricant et à soumettre le traitement de données personnelles du jeu incriminé à un contrôle de conformité à la protection des données. Ces examens sont en cours. Nous informerons le public sur les résultats de ce contrôle le moment venu.

1.3.9 Utilisation des données d´adresses issues de formulaires de contact pour l´évaluation de sites web

Les exploitants de sites web possèdent les données d'adresse des visiteurs qui ont rempli le formulaire de contact pour une communication ou une demande. Il leur vient naturellement l'idée d'utiliser ces adresses pour l'envoi d'un questionnaire d'évaluation du site web. Étant donné que ces données d'adresse sont des données personnelles, une telle utilisation n'est pas admissible d'emblée. Comme nous avons pu le constater dans le cadre d'une demande, les exploitants de sites web ont un certain intérêt à utiliser les données d'adresses collectées par l'intermédiaire du formulaire de contact à d'autres fins. Une utilisation possible est en particulier l'envoi d'un questionnaire permettant d'évaluer le site; toutes les personnes liées à ces adresses ont en effet déjà visité une fois le site en question et peuvent donc donner leur avis sur sa facilité d'utilisation ou sa conception. Les adresses sont par ailleurs déjà disponibles sous forme électronique, ce qui facilite leur utilisation subséquente.

Les visiteurs du site partent quant à eux de l'idée que les informations qu'ils saisissent dans le formulaire de contact sont utilisées uniquement pour le traitement de leur demande. Si ces personnes reçoivent ensuite un questionnaire leur demandant d'évaluer le site, ceci ne suscite pas qu'un mécontentement tout à fait compréhensible; bien plus, un tel envoi est contraire aux principes de la loi sur la protection des données.

Pour éviter cela, les points suivants doivent être pris en considération lors de l'utilisation de ces données à d'autres fins:

- L´exploitant du site doit informer les personnes ayant rempli le formulaire de contact que leurs données peuvent être utilisées à d´autres fins. Il doit mentionner explicitement de quelles fins il s´agit (évaluations, envoi d´informations concernant des produits, etc.). Cette information doit être rédigée sous une forme facilement compréhensible par le public cible et être placée à un endroit bien visible (de préférence sur le formulaire de contact même).
- Chaque utilisateur doit avoir la possibilité d´interdire l´utilisation de ses données personnelles très simplement et gratuitement (option de retrait ou opt-out). Là aussi, la meilleure possibilité consiste à prévoir cela directement sur le formulaire de contact (p. ex. au moyen d´une case qu´il suffit de cocher). Ceci n´exclut pourtant pas que les utilisateurs doivent avoir la possibilité à tout moment d´interdire toute utilisation ultérieure de leurs données.

1.3.10 Intégration de moteurs de recherche étrangers sur les sites web de la Confédération

Toute personne cherchant des informations sur un site web de la Confédération, par exemple dans certains domaines politiques ou des thèmes liés à la santé, doit pouvoir compter sur le fait que les données sur sa personne sont traitées avec le plus grand soin. Les organes fédéraux sont tenus d'accorder une attention particulière aux exigences de protection des données.

La fourniture de services web implique de traiter régulièrement des données personnelles. Ainsi, selon la jurisprudence du Tribunal fédéral, même de simples adresse IP sont considérées comme données personnelles, si l'identification ne nécessite pas de moyens tels que, selon le cours ordinaire des choses, aucun intéressé ne les mettra en œuvre. Par ailleurs, des techniques telles que le recours aux cookies ou l´exploitation de ce que l´on appelle des «referrers» (référants; indications sur l´adresse Internet du site web à partir duquel l´utilisateur a atteint la page actuelle en cliquant sur un lien) permettent souvent d´établir un rapport avec la personne.

La plupart des organes fédéraux proposent des services web et nous les conseillons fréquemment dans ce contexte. La question se pose alors de savoir si les organes fédéraux peuvent intégrer dans leur offre web des moteurs de recherche proposés par des entreprises privées étrangères. Le problème dans le cas examiné résidait dans l´impossibilité d´utiliser la fonction de recherche sans que des informations détaillées sur l´auteur et l´objet de la recherche ne soient transmises à l´entreprise privée domiciliée aux États-Unis. Les algorithmes de recherche reposent précisément sur le fait que ces données (l´adresse IP, mais aussi d´autres identificateurs d´utilisateurs explicites et des indications sur le comportement de recherche, comme les requêtes et les résultats cliqués) sont enregistrées et exploitées. En outre, selon la déclaration de protection des données de l´entreprise privée, les données pouvaient être utilisées à d´autres fins, notamment pour l´amélioration du propre logiciel de l´entreprise permettant l´affichage de publicité personnalisée. L´entreprise concernée exploite des centres de calcul sur l´ensemble du globe. Le nombre de personnes au sein de l´entreprise et les autres services (entreprises tierces privées, autorités étatiques) qui ont le droit ou la possibilité d´accéder à ces données ne sont pas connus et difficilement contrôlables. En raison de la multitude de données ainsi accessibles, ces entreprises sont régulièrement la cible d´attaques pirates du monde entier.

Alors que de telles prestations de services semblent avantageuses à première vue, la médaille a aussi son revers: en divulguant leurs données personnelles et en en perdant le contrôle, les utilisateurs paient finalement un prix élevé.

Depuis le 1er décembre 2010, les autorités fédérales ont une obligation d'informer de manière complète sur leurs collectes de données personnelles. Dans le cas du moteur de recherche de l'entreprise privée américaine que nous avons examiné, ni le but du traitement, ni les catégories de destinataires des données ou les modalités d'exercice du droit d'accès n'étaient suffisamment connus pour pouvoir répondre à l'exigence légale du devoir d'information.

Pour ces raisons, l'intégration de telles fonctions de recherche, proposées apparemment «gratuitement» par des entreprises étrangères, nous semble problématique et pratiquement impossible à mettre en œuvre d'une manière qui soit conforme à la loi.

1.3.11 La surveillance de l'utilisation des moyens d'information et de communication au sein de l'administration fédérale

Il est dans l'intérêt de l'administration fédérale de surveiller l'utilisation des moyens d'information et de communication. Cela doit permettre de garantir l'exploitation des systèmes et d'empêcher les abus. Afin de mener cette surveillance conformément à la loi, les bases légales nécessaires ont été élaborées.

Tout comme dans le secteur privé, il est dans l'intérêt de l'administration fédérale de surveiller l'utilisation des moyens d'information et de communication afin de garantir l'exploitation des systèmes et d'empêcher les abus. Cette surveillance repose en premier lieu sur l'analyse des données générées lors de la connexion. Ces données dites secondaires indiquent par exemple lorsqu'un utilisateur surfe sur Internet quelle adresse IP est entrée en communication avec quel URL (adresse d'un site Internet), quand et combien de temps. Concrètement, ces données permettent d'analyser ultérieurement le comportement d'un collaborateur en matière de navigation sur Internet. Par ailleurs, elles peuvent permettre de trouver par exemple comment un logiciel malveillant (malware) a pu entrer dans le système.

Les données secondaires sont automatiquement générées en tant que données de journalisation (logfiles). Ce sont des données personnelles conformément à la loi sur la protection des données parce qu'elles se rapportent à une personne identifiée ou identifiable. Le traitement de ces données par les organes de la Confédération nécessite donc une base légale (principe de la légalité). Durant l'année sous revue, nous avons participé à un groupe de travail dirigé par l'Office fédéral de la justice qui avait pour but d'élaborer une telle base. Les dispositions fondamentales ont été introduites dans la loi sur l'organisation du gouvernement et de l'administration (LOGA) et les détails ont fait l'objet d'une nouvelle ordonnance (Ordonnance sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération). Les

nouvelles dispositions de la LOGA et de l'ordonnance précitée ont pour but d'établir une réglementation claire d'une part pour l'enregistrement et la conservation des données secondaires (y compris les délais de conservation), d'autre part pour les formes de l'analyse, les conditions qui y sont liées et les principes relatifs aux procédures. Les intérêts légitimes de l'employeur, de l'exploitant du système et de l'employeur ont été ici particulièrement pris en compte.

1.3.12 Les normes de cyberadministration et le nouveau numéro AVS

Il est prévu d'utiliser le nouveau numéro AVS à 13 chiffres, introduit depuis le 1er juillet 2008, comme identificateur de personnes dans certains secteurs de la cyberadministration. Pour cela, une nouvelle «norme eCH» a été créée afin d'en décrire le champ d'application. Nous avons pris position à ce sujet à des fins de clarification et de complément.

L´association eCH promeut, développe et adopte des normes de cyberadministration. Il s´agit d´une coopération entre Confédération, cantons, communes, économie privée et établissements de recherche. Les normes ont valeur de recommandations et leur utilisation au niveau fédéral, cantonal ou municipal peut être rendue obligatoire.

Il est prévu d´introduire l´utilisation du nouveau numéro d´assuré à 13 chiffres de l´AVS comme identificateur commun de personnes dans les registres officiels de personnes des communes, cantons et de la Confédération. Une norme eCH a été élaborée à cet effet en décrivant le champ d´application du nouveau numéro AVS comme identificateur de personne. Lors de l´examen de cette norme, nous avons mentionné séparément les bases légales et les aspects essentiels de l´utilisation du nouveau numéro AVS dans les systèmes de gestion pour donner ensuite une appréciation des utilisations prévues.

La base légale pour une utilisation systématique du nouveau numéro AVS comme identificateur de personnes se trouve dans la loi sur l´AVS. La loi sur l'harmonisation de registres (LHR), de par sa qualité de loi spéciale en matière de droit fédéral, permet qu´il soit utilisé de manière systématique dans certains registres, même en dehors du domaine de l´assurance sociale. Nous avons souligné que cet usage n´est autorisé que s´il correspond au but et au champ d´application définis dans la LHR. Le principal objectif de la loi est de créer une base légale moderne pour l´utilisation des registres de la population cantonale et communale à des fins statistiques.

En conclusion, nous avons retenu que le numéro AVS pouvait être utilisé uniquement dans le champ d´application de la LHR, c´est-à-dire dans le cadre d´analyses statistiques des registres mentionnés dans la loi. Il n´existe aucune base légale permettant

une utilisation généralisée, allant au-delà du domaine de validité de la LHR, dans un système de cyberadministration.

D'autres comptes-rendus sur le nouveau numéro AVS se trouvent aux ch. 1.1.3 et 1.1.4 du présent rapport d´activités.

1.3.13 Avant-projet de l´ordonnance GEVER

Nous avons contribué à l'élaboration de l'avant-projet de l'ordonnance GEVER pour ensuite prendre position sur le sujet dans le cadre de la consultation des offices. L'ordonnance GEVER se fonde juridiquement sur l'article 57h de la loi sur l'organisation du gouvernement et de l'administration, qui stipule que tout organe fédéral peut gérer un système d'information et de documentation à des fins d'enregistrement, de gestion, d'indexation et de contrôle de la correspondance et des dossiers.

Nous avons attiré l´attention en particulier sur la distinction générale entre le système GEVER utilisé pour les processus supra- et intra-départementaux, et les systèmes GEVER des différentes unités administratives de l´administration fédérale. De plus, nous avons souligné à plusieurs reprises qu´une communication de données personnelles au sein d´un système GEVER devait être conforme à l´article 19 de la loi fédérale sur la protection des données (LPD). Dans ce contexte, nous avons mis en évidence l´alinéa 3 de cet article, qui stipule que les organes fédéraux ne sont en droit de rendre des données personnelles accessibles en ligne que si cela est expressément prévu, p. ex. dans une ordonnance. S´il s´agit cependant de données personnelles sensibles ou de profils de la personnalité, l´accès en ligne n´est possible que s´il est explicitement prévu par une loi au sens formel. L´actuelle LOGA ne contient aucune formulation de ce genre. Cela signifie qu´il n´existe à ce jour pas de base légale permettant de rendre accessibles en ligne des données personnelles sensibles ou des profils de la personnalité dans un système GEVER.

1.3.14 Programme GEVER-Bund: traitement des données confidentielles et sensibles

Dans le cadre du groupe de travail concernant les questions de protection des données et de sécurité de l'information, nous avons pu requérir des mesures de sécurité équivalentes pour les documents confidentiels et pour les données sensibles. La nouvelle solution architecturale GEVER proposée constitue une approche pragmatique mais n'apporte pas nécessairement toutes les garanties de confidentialité.

Nous avons participé depuis sa création au groupe de travail concernant les questions de protection et de sécurité des données et les questions de protection et de sécurité de l'information. Le groupe de travail est arrivé à la conclusion que les mesures de sécurité requises pour les documents classifiés confidentiels selon l'Ordonnance concernant la protection des informations de la Confédération (OPrI) et pour les données considérées comme sensibles selon la LPD devaient être équivalentes. Dans un premier temps, un épais catalogue d'exigences techniques destiné aux fournisseurs reconnus de solutions GEVER a été élaboré; celui-ci n'a cependant finalement pas été ratifié par la direction du projet. La nouvelle solution architecturale (SA-GEVER) proposée vise en quelque sorte à compenser l'absence de haute confidentialité dans les systèmes GEVER par un système dual complémentaire couvrant les besoins de chiffrement intra- et inter-GEVER. À noter que le chiffrement envisagé ne concernerait que les quelques documents confidentiels et/ou sensibles. Le chiffrement intra-GEVER serait ainsi assuré par un «Policy Enforcement Point» (PEP) qui contiendrait toutes les clés utiles et dépendrait d'un «Policy Server» géré par l'office concerné. S'agissant du chiffrement inter-GEVER, il est surprenant de constater que la solution proposée recourt à ce même PEP (doté d'une nouvelle «Public Key Infrastructure [PKI]» interdépartementale) en complément de la plateforme SEDEX, plutôt que d'exploiter la solution standardisée «Secure Messaging» (avec son indissociable PKI) désormais disponible auprès de quasi chaque office fédéral. En première analyse, cette approche pragmatique SA-GEVER n'apporte cependant pas nécessairement toutes les garanties de confidentialité par rapport aux administrateurs internes du bénéficiaire de prestations (gérant les PEP et «Policy Server»), ainsi qu'aux prestataires externes de solutions (tous les documents non confidentiels et non sensibles – soit une énorme majorité – ne sont pas chiffrés et donc techniquement lisibles par leur personnel).

1.4 Justice/Police/Sécurité

1.4.1 Mise en œuvre Schengen: contrôle auprès de l'ambassade de Suisse à Moscou

Dans le cadre de la coopération Schengen, notre contrôle auprès de l'ambassade de Suisse à Moscou a permis de se pencher sur différents aspects de protection des données relatifs au processus d'attribution des visas. La gestion des dossiers visas, la méthodologie de recherche des collaborateurs et plus généralement les mesures de sécurité mises en œuvre ont fait l'objet de ce contrôle. Au final, différentes recommandations et propositions d'améliorations ont été adressées à l'ambassade mais également à deux directions du Département fédéral des affaires étrangères.

Le contrôle auprès de l'ambassade de Suisse à Moscou est le quatrième contrôle de ce type que nous avons effectué dans le cadre de la coopération Schengen. Après Le Caire, Kiev et Istanbul, la représentation suisse à Moscou a été choisie au vu du nombre très important de visas délivrés. En effet, si le consulat suisse à Saint-Pétersbourg émet les visas pour la zone nord-ouest du pays, la représentation de Moscou est en charge du reste du pays. Ainsi, environ 63´000 visas ont été émis en 2010. La section visa de l'ambassade collabore avec une entreprise russe externe pour la gestion des rendez-vous. Ce call center est en charge de l'attribution des rendez-vous aux demandeurs individuels.

D'autres demandes de visas sont déposées en groupe par des agences de voyage accréditées en accord avec les autres États membres. Cette manière de faire permet de faciliter le processus d'attribution des visas puisque les agences se chargent de rassembler la totalité des documents nécessaires pour tous les demandeurs et d'effectuer une première vérification pour détecter des documents manquants dans les dossiers des demandeurs.

Après examen de la documentation transmise par la représentation suisse à Moscou, notre visite sur place durant deux jours nous a permis de contrôler les procédures internes en matière d'attribution des visas et de vérifier les mesures de sécurité mises en œuvre. Une visite de l'entreprise externe a également permis de vérifier que les mesures de sécurité nécessaires y étaient appliquées de manière appropriée au regard des exigences formulées dans le cadre de l'accord Schengen.

Lors de la visite sur place, nous avons interrogé les collaborateurs suisses et locaux de la section visa au sujet des différents traitements qu'ils effectuent lors de la procédure d'attribution de visas. Les collaborateurs suisses qui prennent la décision finale

d'accorder un visa ou non ont été plus précisément interrogés sur la méthodologie de recherche qu'ils appliquent lorsqu'ils consultent les banques de données N-SIS et SYMIC, via le masque EVA.

À la suite de la visite sur place, nous avons consulté les logfiles du système N-SIS auprès de fedpol et du système SYMIC auprès de l'ODM afin de vérifier si les accès durant le second jour du contrôle avaient bien été journalisés. De plus, nous avons procédé à une analyse plus approfondie de ces logfiles pour déterminer la plausibilité des requêtes effectuées par les collaborateurs ce jour-là. Nous avons ainsi pu vérifier que la méthodologie de recherche ne posait pas de problèmes.

Nous avons constaté que plusieurs points étaient problématiques et méritaient d'être améliorés. Ainsi nous avons adressé différentes recommandations et propositions d'améliorations à l'ambassade de Suisse à Moscou mais également à deux directions du Département fédéral des affaires étrangères (DFAE) afin qu'il vérifie la conformité de ces points dans l'ensemble de ses représentations à l'étranger. Parmi ces recommandations, certaines s'adressent à l'ambassade et concernent des mesures de sécurité insuffisantes, en particulier par rapport au serveur principal et au partage des locaux avec des collaborateurs du Swiss Business Hub. Nous avons également noté l'absence d'une information suffisante relative aux traitements de données pour les personnes concernées et émis une recommandation. Nous avons recommandé à la direction consulaire du DFAE de vérifier auprès des représentations si le contrat d'externalisation qui lie certaines d'entre elles à des entreprises locales contenait une clause de protection de données. Finalement, comme nous l'avons déjà fait lors d'un précédent contrôle, nous avons adressé à la direction des ressources du DFAE une proposition d'amélioration visant la formation des collaborateurs suisses et locaux au sein des représentations étrangères en matière de protection des données.

1.4.2 Mise en œuvre Schengen: analyse des logfiles du SIS

Les logfiles sont intégrés à la plupart des systèmes informatiques. Ils permettent de garder une trace des différentes actions qui ont été menés dans un système par ses utilisateurs. L'analyse de ces logfiles permet de déterminer lors de contrôles que l'utilisation du système est correcte.

Un logfile est un document qui se présente souvent sous la forme d'un tableur Excel où sont retranscrites les informations nécessaires pour tracer les actions des utilisateurs du système. Nous nous concentrons ici plus particulièrement sur les logfiles du système SIS mais ces considérations sont, pour la plupart, applicables aux logfiles d'autres systèmes également.

Les logfiles du système SIS ont pour but de tracer les recherches qui ont été effectuées par les utilisateurs. Ainsi, les principales informations conservées dans les logfiles SIS sont l'identité de l'utilisateur, la date et l'heure de la recherche ainsi que les données introduites dans le masque de recherche. Les données introduites pour la recherche peuvent être le nom, le prénom ou la date de naissance de la personne recherchée. D'autres informations moins importantes pour l'analyse sont également contenues dans ces logfiles, par exemple des données sur les processus utilisées par le système pour exécuter la requête. Les différentes informations d'un logfile – ou entrées – se présentent habituellement dans un ordre chronologique, mais peuvent être triées différemment.

Lorsque nous procédons, en tant qu'autorité de surveillance, à un contrôle dans le cadre des accords Schengen, nous faisons une demande d'accès aux logfiles du SIS auprès de fedpol. Nous précisons dans ce but la liste des utilisateurs concernés ainsi qu'un intervalle de temps bien défini. La liste et l'intervalle sont définis de façon à ce que l'analyse ultérieure des logfiles reçus soit la plus pertinente possible.

Les logfiles ainsi fournis nous permettent de constater que les requêtes effectuées ont bien été journalisées. Une analyse plus détaillée nous permet de vérifier la plausibilité et la licéité des recherches effectuées par les utilisateurs. En cas de doute, nous procédons à un contrôle plus approfondi en interrogeant directement l'utilisateur concerné sur les raisons qui l'ont poussé à faire la recherche suspecte. L'utilisateur est ainsi confronté aux informations qu'il a introduites dans le masque de recherche et doit se justifier.

Les logfiles du système SIS sont conservés durant une année. Ils sont ensuite détruits et les traces relatives à l'utilisation du système sont perdues.

1.4.3 Groupe de coordination Schengen des autorités suisses de protection des données

Par le biais du «groupe de coordination des autorités suisses de protection des données dans le cadre de la mise en oeuvre de l'accord d'association à Schengen», nous coordonnons avec les autorités cantonales de protection des données nos activités de surveillance des traitements de données effectués en Suisse en matière de migration, police et justice.

Le groupe de coordination des autorités suisses de protection des données s'est réuni le 16 février et le 8 novembre 2011. Lors de ces deux réunions, nous avons informé les autorités cantonales de protection des données des principaux points abordés par l'Autorité de Contrôle Commune (ACC) Schengen et des activités de cette dernière. Nous avons également informé nos collègues cantonaux des résultats de notre

contrôle effectué auprès de la représentation suisse à Moscou. Les cantons quant à eux ont présenté les résultats de leurs activités de contrôle auprès d'utilisateurs cantonaux du SIS. Afin de remédier aux quelques cas d'utilisations abusives du SIS à des fins privées ou de formation, le groupe de coordination a élaboré, en français, allemand et italien, un courrier de sensibilisation à l'intention des services utilisant le N-SIS; ce courrier a été transmis aux autorités fédérales et cantonales concernées.

1.4.4 Droit d'accès direct dans le domaine de la sécurité intérieure (LMSI)

Dans le cadre de la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, le Parlement a décidé de remplacer le droit d'accès indirect par un droit d'accès direct comparable à celui applicable aux systèmes d'information JANUS et GEWA. Pour les autres points que nous avons critiqués, le Parlement a suivi la proposition du Conseil fédéral.

Le Parlement a arrêté en décembre 2011 une modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Contrairement au projet du Conseil fédéral qui prévoyait le droit d'accès direct en application des articles 8 et 9 de la loi fédérale sur la protection des données (LPD), le Parlement, après élimination des divergences entre les deux Conseils, a décidé la mise en place d'un droit d'accès direct basé en grande partie sur la législation régissant l'accès aux systèmes d'information JANUS et GEWA telle que prévue dans la loi fédérale sur les systèmes d'information de police de la Confédération (LSIP).

Dans le cadre de cette nouvelle réglementation, les demandes d'accès doivent être déposées auprès du Service de renseignement de la Confédération (SRC). Celui-ci peut différer sa réponse dans trois cas:

- Les données traitées concernant le requérant sont liées à des intérêts prépondérants qui exigent le maintien du secret dans le cadre de la détection précoce et de la lutte contre les dangers en matière de terrorisme, de service de renseignement prohibé, d'extrémisme violent, des actes préparatoires relatifs au commerce illicite d'armes et de substances radioactives et du transfert illégal de technologie ainsi que dans le cadre d'une poursuite pénale ou d'une autre procédure d'instruction.
- Les intérêts prépondérants d'un tiers l'exigent.
- Aucune donnée concernant le requérant n'est traitée.

Dans ces trois cas, le SRC informe le requérant du report de sa réponse et lui indique qu'il peut nous demander de vérifier la licéité du traitement et l'existence d'intérêts prépondérants justifiant le report. Nous procédons aux vérifications demandées et indiquons au requérant qu'aucune donnée le concernant n'est traitée illégalement ou qu'en cas d'erreur relative au traitement des données ou au report de la réponse, une recommandation a été adressée au SRC. Nous informons également le requérant de la possibilité de saisir le Tribunal administratif fédéral (TAF) afin que celui-ci vérifie sa communication ou l'exécution de l'éventuelle recommandation qu'il a émise. Le TAF effectue la vérification demandée et en informe le requérant. En cas d'erreur, le TAF adresse au SRC une décision lui ordonnant d'y remédier. Le SRC communique au requérant les renseignements qu'il a demandés dès que les intérêts liés au maintien du secret ne peuvent plus être invoqués, mais au plus tard après l'expiration du délai de conservation. Pour le requérant qui n'est pas enregistré, le SRC l'informe au plus tard trois ans après réception de la demande. Exceptionnellement, nous pouvons recommander au SRC de fournir immédiatement le renseignement demandé pour autant que cela ne menace pas la sûreté intérieure ou extérieure. Cette nouvelle réglementation nécessite encore un certain nombre de précisions quant à son application pratique.

En ce qui concerne l'ancrage dans la LMSI des normes figurant dans l'ordonnance concernant l'extension du devoir de renseigner et du droit de communiquer d'autorités, d'offices et d'organisations visant à garantir la sécurité intérieure et extérieure, le Parlement n'a pas tenu compte de nos remarques (cf. notre 18e rapport d'activités 2010/2011, ch. 1.4.6).

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

En 2011, le nombre des demandes d'accès concernant le système d'information ISIS a été le troisième plus important depuis 1998. En décembre, le Parlement a décidé l'introduction d'un droit d'accès direct comparable à celui qui est applicable aux systèmes d'information JANUS et GEWA.

En 2011, 66 demandes d'accès indirect concernant le système d'information ISIS ont été déposées auprès de notre secrétariat. Ce nombre est le troisième plus important depuis 1998. En 2010, 410 demandes avaient été examinées (cf. notre 18e rapport d'activités 2010/2011, ch. 1.4.7) et en 2008, 148 demandes avaient été traitées (cf. notre 16e rapport d'activités 2008/2009, ch. 1.4.4).

Le Parlement a arrêté le 23 décembre la modification de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Dans ce cadre, l'article 18

relatif au droit d'accès a été modifié; la nouvelle réglementation introduit un droit d'accès direct comparable à celui qui est applicable aux systèmes d'information JANUS et GEWA.

Pour plus de détails concernant cette nouvelle réglementation, voir le ch. 1.4.4.

1.4.6 Essai pilote du système d'information ISAS

La base juridique régissant l'essai pilote ISAS a été adaptée afin de refléter la situation réelle et non celle de l'exploitation définitive envisagée. Une liste exhaustive des champs de données doit être définie aussi pour un essai pilote. Ainsi le Conseil fédéral et le Département fédéral de la défense, de la protection de la population et des sports ont modifié deux ordonnances concernant l'essai pilote ISAS.

Nous avons demandé au Service de renseignement de la Confédérations (SRC) de nous transmettre un rapport intermédiaire concernant l'essai pilote ISAS (cf. notre 18e rapport d'activités 2010/2011, ch. 1.4.8). Nous avons émis des remarques concernant ce rapport, notamment sur deux points importants.

Premièrement, nous avons constaté que la situation réelle de l'essai pilote ne correspondait pas à la base juridique. Celle-ci mentionnait que le système d'information ISAS était composé de plusieurs banques de données. Dans la réalité, ISAS n'est qu'une seule banque de données. Nous avons donc demandé au SRC d'adapter la conception informatique pour respecter la base juridique en vigueur ou de modifier cette dernière afin de refléter la situation réelle de l'essai pilote ISAS. Le SRC a choisi d'adapter la base juridique.

Deuxièmement, les différents champs de données ne figuraient pas dans la base juridique. On y trouvait à la place une description du modèle de la banque de données utilisée. De plus, cette banque de donnée était conçue de telle manière que des champs de données pouvaient être définis par les utilisateurs. Cette solution qui permet de définir les champs de données durant la phase pilote n'est pas conforme aux exigences de la protection des données. En effet, l'institution de l'essai pilote permet que le traitement de données personnelles sensibles ou de profils de la personnalité soit réglé par une base légale provisoire de niveau inférieur. Toutefois, les champs de données doivent être fixés de manière exhaustive comme pour l'exploitation définitive d'un système d'information. S'il apparaît au cours de l'essai pilote que de nouveaux champs de données sont nécessaires, la disposition mentionnant les champs de données doit être modifiée. En conséquence, nous avons demandé au SRC d'établir une liste exhaustive des champs de données du système d'information ISAS et de l'intégrer dans la base juridique régissant l'essai pilote, ce qu'il a fait.

La modification de l'Ordonnance sur les systèmes d'information du Service de renseignement de la Confédération (OSI-SRC) est entrée en vigueur le 1er janvier 2012; l'ordonnance décrit enfin l'essai pilote ISAS tel qu'il est et non tel qu'il pourrait être lors de l'exploitation définitive du système d'information. À la même date est entrée en vigueur une modification de l'ordonnance du DDPS sur les champs de données et les droits d'accès aux systèmes d'information ISAS et ISIS. Cette modification concerne notamment la liste exhaustive des champs de données du système d'information ISAS.

1.4.7 Demandes de vérification concernant le N-SIS et les systèmes d'information JANUS et GEWA

Nous recevons en moyenne par année sept demandes de vérification concernant les systèmes d'information JANUS et GEWA. Pour la partie nationale du système d'information Schengen, les autorités européennes de protection des données nous ont adressé 15 demandes de vérification et trois personnes ont déposé des demandes semblables depuis l'entrée de la Suisse dans l'espace Schengen.

Dans le cadre des demandes d'accès aux systèmes d'information JANUS et GEWA, la loi fédérale sur les systèmes d'information de police de la Confédération prévoit que l'Office fédéral de la police (fedpol) diffère sa réponse si les données concernant le requérant sont liées à des intérêts prépondérants pour la poursuite pénale qui exigent le maintien du secret ou si le requérant n'est pas enregistré. Dans ces deux cas, fedpol informe le requérant du report de sa réponse et lui indique qu'il peut demander au Préposé fédéral à la protection des données et à la transparence (PFPDT) qu'il vérifie si les éventuelles données le concernant sont traitées conformément au droit et si des intérêts prépondérants liés au maintien du secret justifient le report. Depuis l'entrée en vigueur le 5 décembre 2008 de la loi susmentionnée, nous avons reçu 22 demandes de vérification (5 en 2009, 12 en 2010 et 5 en 2011).

La législation applicable à la partie nationale du système d'information Schengen (N-SIS) stipule que toute personne a le droit de demander aux autorités de contrôle de vérifier les données la concernant intégrées dans le N-SIS ainsi que l'utilisation qui est faite de ces données. Depuis l'entrée de la Suisse dans l'espace Schengen le 12 décembre 2008, trois personnes nous ont demandé de procéder à des vérifications dans le N-SIS. Durant cette même période, nous avons reçu de nos collègues européens 15 demandes de vérification. Nous avons également reçu plusieurs demandes de vérification provenant de personnes résidant à l'étranger. Ces demandes correspondaient plus à des demandes d'accès au N-SIS plutôt qu'à des demandes de vérification. Nous

avons transmis ces demandes à fedpol et avons informé les personnes concernées que le droit d'accès au N-SIS est un droit d'accès direct en Suisse et que les demandes doivent ainsi être adressées directement au gestionnaire du N-SIS, à savoir fedpol.

1.4.8 Réglementation plus claire pour la surveillance de la correspondance par poste et télécommunication (LSCPT)

Nous avons, dans le cadre de la consultation des offices, pris position sur la révision partielle de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication, ainsi que sur les résultats de la procédure de consultation concernant la révision totale de la loi fédérale; nous avons à cette occasion également donné notre avis sur l'utilisation des chevaux de Troie gouvernementaux.

La surveillance de la correspondance par poste et télécommunication par les autorités de poursuite pénale a été largement débattue dans les médias l'an dernier, en particulier la surveillance à l'aide de programmes du type «GovWare» (dits «chevaux de Troie gouvernementaux»). Nous nous sommes prononcés à ce sujet dans le cadre de la consultation des offices sur la révision partielle de l'ordonnance sur la surveillance de la correspondance par poste et télécommunication (OSCPT) et avons signalé notamment que la terminologie concernant le champ d'application devait être harmonisée avec celle de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT). Cela permettrait de mieux circonscrire les fournisseurs d'accès Internet et les fournisseurs de services de télécommunication soumis à l'OSCPT. De plus, nous avons demandé que le cercle des prévenus soit déjà défini dans l'ordonnance de manière plus claire par l'intégration de critères de recherche. Cette objection que nous avons émise à propos de la recherche par champ d'antennes a été rejetée dans la proposition au Conseil fédéral et devrait être réexaminée dans le cadre de la révision déjà amorcée de la LSCPT.

Nous avons été invités par la Commission des affaires juridiques du Conseil national à nous prononcer sur l'utilisation de programmes de type GovWare en matière de poursuite pénale. À cette occasion, nous avons attiré l'attention sur le fait que les atteintes aux droits fondamentaux nécessitent une base légale formelle et matérielle qui, en outre, doit être formulée avec suffisamment de précision. Cela vaut, en raison de ses multiples possibilités de configuration, à la fois pour les fonctionnalités du logiciel que pour les exigences attachées à la demande de surveillance et pour la liste des infractions. Il nous semble important, dans la perspective des tâches des autorités de poursuite pénale, de créer une base légale claire régissant l'utilisation des logiciels en vue de poursuivre les infractions graves, y compris le débat public qui accompagne le sujet. Cette base légale doit être créée en parallèle à la révision totale de la LSCPT en cours.

1.4.9 Formation au Service de renseignement de la Confédération

Nous avons eu l'occasion d'organiser une séance de formation continue auprès du Service de renseignement de la Confédération en collaboration avec la conseillère en matière de protection des données. Nous avons commencé par donner aux collaborateurs un aperçu général sur la protection des données, pour aborder ensuite les aspects théoriques et pratiques du droit d'accès.

En collaboration avec la conseillère en matière de protection des données du Service de renseignement de la Confédération (SRC), nous avons élaboré le module «Protection des données» destiné à la formation continue des collaborateurs. Ce module, intitulé «Droit d´accès direct et indirect – Théorie et pratique», a pu être présenté en tout six fois, soit quatre fois en allemand et deux fois en français. Dans la première partie, nous avons exposé aux participants les principes généraux de la loi sur la protection des données en soulignant que chacun se trouve quotidiennement confronté à des questions de protection des données. Nous avons cité comme exemples le traitement de données personnelles par les sociétés de renseignement commercial, dans le domaine de la santé, lors de la surveillance vidéo, par les entreprises lorsqu´elle utilisent des données clients ou par les organes fédéraux, p. ex. pour la gestion du registre automatisé des autorisations de conduire.

L´élément principal du module traitait du droit d´accès. Après avoir donné quelques précisions sur le droit d´accès direct selon la loi sur la protection des données, nous avons abordé le droit d´accès indirect, tel qu´il existe encore actuellement dans le cadre du système d´information ISIS du SRC et avons expliqué comment nous procédons en pratique pour la vérification de ces demandes d´accès indirectes. Ensuite, la conseillère en matière de protection des données du SRC a exposé comment le SRC procède pour fournir les renseignements aux personnes enregistrées qui ont déposé une demande d´accès, une fois que les éventuels intérêts de maintien du secret liés à la sûreté intérieure ont été écartés.

Pour clore, nous avons exposé comment le droit d´accès est réglé au sein de la Police judiciaire fédérale pour le système de traitement des données relatives aux infractions fédérales. La séance a été suivie d´un bref résumé des délibérations du Tribunal fédéral sur l´arrêt du 2 novembre 2011 concernant une demande d´accès indirecte, ainsi qu´une remarque sur les débats au Parlement concernant la révision du droit d´accès auprès du SRC. Entretemps, le Parlement a adopté une réglementation analogue à celle du système de traitement des données relatives aux infractions fédérales pour le système d'information sécurité intérieure ISIS (cf. ch. 1.4.4 du présent rapport d´activités).

1.5 Santé et recherche

1.5.1 SwissDRG: révision de la loi et de l'ordonnance sur l'assurance maladie

Dans le système SwissDRG, la facturation des prestations ambulatoires dans le domaine des soins somatiques aigus nécessite la réglementation des transmissions des données relatives à la santé. La conformité de celle-ci avec la protection des données constitue un défi de taille pour tous les participants. Après l'échec des conventions tarifaires, une solution légale doit désormais être trouvée.

Le nouveau financement des hôpitaux est entré en vigueur le 1er janvier 2012. Les montants forfaitaires en fonction du diagnostic (en anglais Diagnoses Related Groups, soit DRG) sont la clé de voûte de ce nouveau système dans le domaine des soins ambulatoires et somatiques aigus. S'inspirant du système allemand, la Suisse a mis sur pied le SwissDRG.

Conformément au système de santé applicable en Suisse, les partenaires tarifaires (l'Association faîtière des assurances maladie santésuisse, l'Association suisse des hôpitaux H+ et la Conférence suisse des directrices et directeurs cantonaux de la santé, la CDS) auraient dû s'accorder aussi, dans le cadre d'une structure tarifaire valable pour toute la Suisse et approuvée par le Conseil fédéral, sur la transmission des données relatives aux diagnostics et aux procédures afin de contrôler les factures dans le cadre de la facturation. Cette convention aurait permis de garantir, conformément au principe de la proportionnalité fixé dans le droit de la protection des données et à la jurisprudence du Tribunal administratif fédéral, que les assureurs-maladie ne reçoivent que les données dont ils ont besoin pour le contrôle des factures. Dès juillet 2009, les partenaires tarifaires avaient adopté une structure tarifaire également approuvée par le Conseil fédéral. Toutefois, ce dernier avait maintenu que justement la transmission de données concernant les diagnostics et les procédures n'était pas encore suffisamment réglementée et demanda aux parties d'améliorer encore cette structure tarifaire.

Manifestement, les négociations avec les partenaires tarifaires, auxquelles nous n'avons bien entendu pas participé et dont le déroulement ne nous a été communiqué qu'indirectement, ont longuement piétiné. Nous avons eu l'impression que les questions de protection des données étaient mêlées aux questions financières. Enfin, les partenaires tarifaires se sont mis d'accord sur une convention additionnelle. Mais en août 2011, au terme d'une votation interne, les membres de l'Association suisse des hôpitaux H+ ont refusé cette convention. Comme un règlement amiable entre les partenaires tarifaires n'était plus envisageable dans un délai raisonnable et qu'il fallait

barrer la route à une multitude de réglementations cantonales éventuellement différentes, le Département fédéral de l'intérieur (DFI), compétent en la matière, est alors intervenu et a déclaré qu'il allait réglementer la transmission des données dans la loi. La modification de la loi fédérale sur l'assurance-maladie (LAMal) oblige désormais les fournisseurs de prestations à mentionner de manière codée sur la facture les diagnostics et les procédures. Les détails concernant la transmission des données seront réglés par le Conseil fédéral dans l'ordonnance sur l'assurance-maladie (OAMal), conformément au principe de la proportionnalité. Nous avons étroitement collaboré à cet égard avec le Secrétariat général du DFI et présenté des propositions de solution. En résumé notre requête est la suivante: l'assureur reçoit les données qui lui sont vraiment nécessaires; en outre, il doit être garanti qu'au sein de l'assurance, seules les personnes qui en ont vraiment besoin ont accès à ces données très sensibles. Ce point doit être garanti par les assureurs sur la base de mesures techniques et organisationnelle appropriées comme les techniques de cryptage et doit être régulièrement contrôlé. Il faut surveiller de près l'évolution concernant le système SwissDRG. La création d'une centrale indépendante de compensation pour le contrôle des factures demeure une alternative sérieuse au système actuel.

1.5.2 Loi fédérale sur le dossier électronique du patient

Dans le cadre de la consultation des offices, nous avons pris position sur l'avant-projet de la nouvelle loi fédérale sur le dossier électronique du patient. Celle-ci réglemente des aspects importants telles que l'accès aux dossiers électroniques des patients. À notre demande, certaines exigences clés de la protection des données ont été prises en compte dans le projet de loi qui a été mis en consultation fin 2011.

Le dossier électronique du patient représente l´élément central de la cybersanté. C´est un dossier virtuel permettant de rendre accessibles en ligne des données enregistrées de manière décentralisée qui sont pertinentes pour le traitement d'un patient ou d´une patiente. Il s'agit en l´occurrence de données personnelles sensibles. Leur traitement doit être réglementé de manière concrète et contraignante. Pour cette raison, nous avons demandé que les exigences de protection et de sécurité des données soient explicitement mentionnées dans la loi comme conditions requises pour une certification.

En ce qui concerne le règlement du consentement, nous avons demandé que ce dernier ne soit valable que s´il a été donné de plein gré et que la personne concernée a été suffisamment informée sur la nature du traitement des données et de ses effets. Le projet de loi a été adapté en conséquence.

Par identificateurs on entend les caractéristiques personnelles qui rendent une personne identifiable. L´authentification permet de vérifier qu´une personne est vraiment celle qu´elle prétend être. Une fois authentifiée avec succès, la personne peut être autorisée à accéder à ses données. La qualité du processus dépend entièrement de la qualité de l´identificateur. Si ce dernier contient des caractéristiques inappropriées, il se peut que l´attribution à une personne ne soit pas univoque. La Centrale de compensation (CdC), qui a mis en service le nouveau numéro AVS (NAVS13) présume elle-même que 200'000 personnes environ ont reçu plus d´un numéro NAVS13. C´est pourquoi la CdC recommande de combiner le numéro AVS avec au moins cinq autres caractères d´identification. Nous partageons cet avis.

En outre, nous demandons que le numéro NAVS13 ne permette pas, ni directement ni indirectement, d´établir une relation avec des données de santé. Ceci parce que leur utilisation de plus en plus fréquente dans l´administration (fédérale et cantonale) mène à de nombreuses corrélations avec d´autres fichiers. Selon le projet de loi, le Conseil fédéral peut prévoir que des communautés certifiées puissent utiliser le numéro d´assuré comme caractère d´identification des patients. Pour ce cas, nous recommandons de transformer le numéro NAVS13 de manière systématique de sorte qu´il puisse être utilisé comme identificateur sectoriel.

1.5.3 Saisie systématique des dossiers par la SUVA

Un examen des faits a montré que la SUVA avait pris les mesures requises par la saisie systématique des dossiers et qu'en règle générale, le droit d'accès peut aussi être garanti conformément à la loi sur la protection des données

Un avocat nous a écrit pour nous signaler certaines incohérences concernant un dossier géré par la SUVA. Dans le cadre d'un contentieux judiciaire, il avait effectué sur mandat d'un client plusieurs demandes de consultation de dossier conformément à l'art. 46 de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA). Il avait constaté ce faisant que le volume du dossier variait et que les documents reçus étaient en partie numérotés de manière différente. Étant donné que la saisie systématique de dossiers constitue une condition de base pour pouvoir garantir le droit d'accès conformément à la loi fédérale sur la protection des données, nous avons procédé à une clarification des faits. L'objectif n'était pas de tirer au clair le cas dénoncé par l'avocat, mais d'examiner d'une manière générale si la SUVA veillait véritablement à la saisie systématique des dossiers.

Notre constatation de l'état de fait nous a permis d'établir que divers points pouvaient influencer de manière négative la saisie systématique des documents et en particulier

leur numérotation cohérente: d'une part, en cas de contentieux judiciaire entre une personne assurée et la SUVA, l'agence compétente doit transmettre le dossier original au service juridique du siège principal de la SUVA à Lucerne pour que ce dernier puisse le remettre au tribunal. Ainsi, seules des copies demeurent auprès de l'agence compétente et du service juridique du siège principal. D'autre part, la SUVA se trouve actuellement dans une phase transitoire entre dossiers sur papier et traitement électronique du courrier entrant. Ainsi, dans certains cas, c'est à l'agence compétente de décider quel est le dossier déterminant (dossier papier ou électronique). Justement lorsqu'elles se combinent comme dans le cas dénoncé par l'avocat, ces circonstances constituent des sources potentielles d'erreurs. Notre clarification des faits a toutefois montré que la SUVA a aussi pris durant cette phase de transition les mesures fondamentales requises pour la garantie d'une saisie systématique des dossiers. Nous n'avons pas été obligés d'émettre une recommandation.

1.5.4 Examen des faits auprès de la SUVA

Nous avons procédé à un examen des faits auprès de la SUVA dans le domaine de la gestion des cas. Cet examen a révélé que la gestion des cas ne soulève en soi pas de problèmes de protection des données. Nous avons cependant identifié des lacunes dans la gestion des droits d'accès aux données des personnes assurées. La SUVA a reconnu le problème et pris des mesures immédiates pour réduire le nombre de personnes autorisées.

Dans le cadre d´un examen des faits effectué à la SUVA, nous avons entre autres examiné le concept des rôles et des droits d´accès. Celui-ci prévoit quatre niveaux de droits d´accès: l´accès des collaborateurs aux dossiers de leur propre agence, celui aux dossiers gérés dans d´autres agences, l´accès des collaborateurs de certains services (p. ex. le service juridique) et l´accès aux dossiers concernant les accidents de travail. Nos recherches ont révélé qu´un nombre disproportionnellement élevé de collaborateurs disposait d´un droit d´accès aux dossiers gérés dans les autres agences. Bien que cette autorisation n´était accordée à un collaborateur seulement en cas de nécessité pour le traitement d´un dossier, elle n´était ensuite pas annulée lorsque l´accès n´était plus requis. Une autre lacune du concept de la SUVA est que les autorisations d´accès s´appliquent à tous les dossiers d´une agence.

La Direction de la SUVA a engagé une première mesure immédiate ayant pour objet une réduction des autorisations d´accès à des dossiers externes aux agences. Les employés perdent leur droit d´accès aux agences externes dès qu´ils n´en ont plus besoin. La mesure s´inscrit dans le cadre d´un large remaniement du concept des rôles et des

droits d´accès. En été 2012, nous procéderons conjointement avec la SUVA à une analyse des résultats suivie d´une évaluation critique.

Ce cas est un exemple classique de violation de la protection des données causée par une lacune systématique au niveau du concept des droits d´accès. Si l´on édicte bien des règles pour l´attribution des rôles et des autorisations d´accès, on omet toutefois de réglementer la modification du rôle ou de l´autorisation. Il en résulte une collection absolument démesurée de droits d´accès constituée au fil du temps. Une procédure d´attribution de droits d´accès doit donc toujours être accompagnée d´une procédure correspondante pour le retrait de ces droits.

1.5.5 Circulaire 7.1 de l´Office fédéral de la santé publique

L'Office fédéral de la santé publique a envoyé en août 2011 une circulaire à tous les assureurs-maladie. À notre avis, celle-ci contient quelques points problématiques, notamment en ce qui concerne le projet des règlements de traitement, le suivi des données relatives au diagnostic et la gestion des cas.

En août 2011, l´Office fédéral de la santé publique (OFSP) a envoyé à tous les assureurs-maladie du domaine obligatoire une circulaire intitulée «Assureurs-maladie: organisation et processus conformes à la protection des données». Son but était de rappeler aux assureurs les principes et les prescriptions en vigueur en matière de protection des données. Elle a également attiré l´attention sur l´entrée en vigueur et l´application de nouvelles dispositions de la loi sur l'assurance-maladie (LAMal).

Nous aimerions relever quelques points qui ont suscité notre étonnement: la circulaire explique dans un premier temps que les assureurs-maladie ne sont pas tenus de payer les fournisseurs de prestations s´ils ne reçoivent pas de facturation détaillée. Ce qui nous a le plus étonnés est que cette circulaire a été envoyée par l´OFSP en été dernier, alors que l´introduction de SwissDRG était imminente et que le transfert de données entre les fournisseurs de prestations et les assureurs-maladie allait, dans le cadre de ce système-là, être réglé par une nouvelle ordonnance. La circulaire traite également de la gestion des cas. Elle ne répond cependant pas à la question de savoir à qui les gestionnaires de cas sont subordonnés et à quelles données ils ont accès. Il est nécessaire à notre avis que les données traitées par les gestionnaires de cas ne se retrouvent pas dans le dossier qui est également accessible aux autres collaborateurs, après liquidation du cas. Le consentement à la gestion des cas ne peut pas, à notre avis, être considéré comme une extension de l´autorisation légale à traiter les données.

Un point précis de la circulaire a également des conséquences pour nous: l´entrée en vigueur de l´article 84b LAMal nous concerne dans la mesure où les assureurs-maladie doivent, dès le 1er janvier 2012, spontanément nous remettre leur règlement de traitement pour appréciation. Mais, comme nous l'avons déjà expliqué à la commission compétente avec des propos repris expressément par la conseillère d'État Erika Forster-Vannini lors de la réunion de la Chambre du 6 décembre 2007, nous ne disposons actuellement pas des ressources humaines nécessaires pour examiner de manière systématique tous les règlements de traitement des assureurs-maladie admis selon la LAMal. Nous procéderons plutôt à des contrôles aléatoires en fonction des ressources disponibles et des priorités que nous avons fixées. Les assureurs-maladie étant des organes fédéraux selon la LAMal, ils ont aujourd'hui déjà, en raison de l'ordonnance relative à la loi fédérale sur la protection des données (OLPD), l'obligation de prendre les mesures techniques et organisationnelles nécessaires pour protéger la personnalité et les droits fondamentaux de la personne dont ils traitent des données. Ils doivent également tenir un règlement de traitement des données pour chaque fichier automatisé qu'ils exploitent, le tenir à jour et nous le mettre à disposition. En ce sens, l'article 84b ne fait que répéter et préciser des obligations légales existantes. Ce qui est par contre nouveau, c'est qu'à partir du 1er janvier 2012 les assureurs-maladie doivent, en vertu de l'article 84b LAMal, publier leurs règlements de traitement. Cette obligation est indépendante d'une éventuelle appréciation que nous aurions faite.

Si nous évaluons le règlement de traitement d'un assureur-maladie, ceci se fera sous la forme d'un examen des faits selon l'article 27, al. 2 LPD. L'assureur-maladie concerné en sera évidemment informé par écrit. Si une recommandation est nécessaire, nous sommes de toute façon obligés d'informer le Département fédéral de l'intérieur (DFI) en tant que département compétent. Nous pouvons très bien imaginer informer en même temps l'OFSP et nous souhaiterions que ce dernier nous informe des problèmes qu'il a identifiés lors de ses audits auprès des assureurs-maladie.

En ce qui concerne la validité d'un règlement de traitement, nous tenons à préciser ce qui suit: Même l'article 84b de la LAMal ne nous a pas conféré la compétence de procéder à des enquêtes préliminaires concernant de tels faits.Les assureurs-maladie admis selon la LAMal sont tenus en tant qu'organes fédéraux d'élaborer un règlement de traitement qui réponde aux exigences légales. Un règlement de traitement des données est considéré comme valide dès qu'il a été accepté et déclaré obligatoire par l'assurance concernée, même sans notre appréciation.

1.5.6 Transmission de données à un centre de recherches par les services de soins à domicile

Par une fonction à sens unique (fonction de hachage), à partir de données identifiantes, il est possible de générer un code numérique qui permet de fournir des données sous forme pseudonymisée à des fins de recherche ou d'assurance qualité.

Aujourd´hui, la plupart des services d´aide et de soins à domicile utilisent des systèmes d´information modernes pour traiter de manière efficace les données des personnes dont ils s´occupent. Ces données peuvent également être utilisées à des fins d´assurance qualité ou pour la recherche. Cela implique que les divers services d'aide et de soins à domicile exportent leurs données dans une base de données centrale. Pour des raisons de protection des données, il faut veiller à ne transmettre que des données anonymes. Le déroulement implique que les données des personnes prises en charge, saisies au fil du temps, soient correctement attribuées aux données existantes dans la base centrale. Ceci a été réalisé à l´aide d´une fonction à sens unique (ou fonction de hachage). Cette fonction permet, en partant des mêmes données initiales (code numérique unique complété par un code supplémentaire [Salt] pour augmenter la sécurité), de générer un pseudonyme qui peut en tout temps être reconstitué sur la base des données initiales de la personne. L´opération inverse, à savoir retrouver les données initiales à partir du pseudonyme, n´est par contre pas possible. Une telle démarche garantit l´anonymat des personnes prises en charge, étant donné qu´aucune autre donnée identifiante telle que nom ou adresse n´est transmise.

En outre, il est important que les champs de données transmis avec le pseudonyme à la banque de données centrale pour l´assurance qualité ou la recherche soient analysés quant à la présence de données identifiantes. Lors de cette analyse, nous avons remarqué que l´indication de la profession alliée à la date de naissance de la personne pouvait se révéler délicate étant donné qu´elle peut permettre, pour les professions ou fonctions rares, d´identifier la personne en question. Dans de tels cas, il est donc indispensable de ne pas saisir la dénomination de la profession ou d´utiliser une dénomination plus générale.

1.5.7 La transmission des données dans le cadre d´essais cliniques

Les essais cliniques confrontent les services concernés à des problèmes délicats du point de vue de la protection des données lorsqu'ils utilisent les données personnelles de patients à la fois pour leur traitement et pour la recherche. Nous sommes intervenus en faveur de solutions appropriées.

Pour les essais sur le plan international, Swissmedic a décidé en 2010 de ne pas accepter de cahiers d´observation («Case Report Forms») contenant des données personnelles des sujets qui prennent part aux essais cliniques. Cette décision était fondée sur une prise de position de notre part, dans lequel nous avions, à la demande de Swissmedic, expliqué quelles sont les exigences envers une pseudonymisation acceptable du point de vue de la protection des données.

Suite à la décision susmentionnée de Swissmedic, une commission cantonale d´éthique a suspendu sa prise de position sur un essai clinique d´un groupe de recherche. Ce groupe a alors fait appel à nous afin de trouver une solution conforme à la protection des données pour les essais thérapeutiques en oncologie pédiatrique. Ces essais sont menés dans des circonstances particulières: ils portent en moyenne sur trois ou quatre patients en Suisse, au maximum 40. En raison du nombre limité d´enfants souffrant de tumeurs rares, le diagnostic et le traitement ne peuvent être optimisés que si l´on travaille en étroite collaboration avec des institutions étrangères. Les chercheurs ont fait valoir qu´il était nécessaire, pour des raisons de sécurité du patient, de communiquer le nom complet et la date de naissance lors des demandes ou entretiens.

Nous avons organisé une réunion avec des représentants du groupe de recherche et de Swissmedic afin de trouver une solution appropriée et conforme à la protection des données. Dans une prise de position rédigée à l´issue de cette réunion, nous nous sommes exprimés sur les exigences en matière de protection des données. Comme point de départ, nous avons pris la définition de l´objectif poursuivi par les traitements de données prévus. Dans le cas présent, il s´agissait de deux objectifs: d´une part, une amélioration du diagnostic et du traitement des personnes participant à l´essai, d´autre part, la recherche à l´aide des constats obtenus. À notre avis, les conditions suivantes devraient être remplies:

- Dans la première phase d´un essai clinique, les divers services traitants peuvent, dans les conditions particulières susmentionnées, être considérés comme une seule équipe élargie de traitement. La transmission de données personnelles au sein de cette équipe élargie est admissible, pour autant que les dispositions

légales applicables soient respectées. Les acteurs doivent notamment veiller à ce que les données soient transmises de manière sécurisée et qu'elles soient accessibles uniquement aux interlocuteurs autorisés.

- Le concept des essais doit clairement mentionner les différentes phases de l´essai clinique. Le consentement des sujets doit porter sur toutes les phases de l´essai.
- Le concept des essais doit également montrer à quel moment on passe du traitement à la recherche. Lors de cette transition, les données personnelles doivent être anonymisées.
- En ce qui concerne le contexte européen de l´essai, les parents ou les enfants doivent donner leur consentement pour la communication des données à l´étranger. Si les données transmises par la Suisse à des institutions étrangères sont plus tard utilisées par celles-ci à des fins propres (p. ex. pour constituer leur propre base de données de recherche), les personnes concernées doivent également donner leur consentement.

1.5.8 Système boule de neige dans la recherche

Nous avons procédé à un examen des faits à l'EPF de Zurich concernant un projet de recherche. La collecte des données d'adresses utilisées pour contacter de nouveaux participants au projet de recherche fonctionnait selon le système «boule de neige».

Au cours de l'année sous revue, nous avons effectué un examen des faits à l´EPF de Zurich. Celui-ci fut motivé par un projet de recherche qui examinait les réseaux sociaux en mettant l´accent sur le comportement en matière de mobilité. Le recrutement de nouveaux participants se faisait selon un système «boule de neige», en suivant le réseau social des personnes interrogées. Ainsi, les participants communiquaient aux chercheurs les coordonnées de leurs connaissances ainsi que certaines informations complémentaires. Ces nouveaux contacts étaient par la suite informés sur le projet par les chercheurs et étaient à leur tour invités à y participer.

Après avoir dans un premier temps informé l´une des personnes concernées sur ses droits, nous avons l´an dernier été contactés par l´EPF de Zurich suite à la diffusion d´un reportage télévisé. Nous avons alors décidé de procéder à un examen des faits. Nous avons constaté que les collaborateurs impliqués de l´EPFZ sont sensibilisés aux aspects de la protection des données et qu'ils s´efforcent de respecter les prescriptions légales applicables. Ainsi, certaines de nos propositions ont été mises en œuvre immédiatement, par exemple au niveau du contrôle de l´accès aux données de recherche.

En ce qui concerne les bases légales, notre examen a fourni un résultat surprenant. Normalement, un organe fédéral doit pouvoir s´appuyer sur des dispositions légales pour traiter des données personnelles sensibles ou des profils de personnalité. La loi sur la protection des données privilégie cependant le domaine de la recherche par des exigences de traitement moins sévères dans certains cas. Pour les faits que nous avons analysés, cela signifie concrètement que l´EPFZ aurait besoin de telles dispositions dans une ordonnance. Les directives internes sur l´intégrité dans le domaine de la recherche édictées pour les collaborateurs ne répondent pas à ces exigences formelles. Les travaux législatifs que nous avons proposés concernent l´ensemble de l´EPFZ. Celle-ci a donc pris contact avec le Conseil des EPF à ce sujet, et le travail législatif a été entamé en collaboration avec l´Office fédéral de la justice.

1.6 Assurances

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

La loi sur le contrat d'assurance fait l'objet d'une révision totale. Le projet présenté au Parlement prévoit enfin d'ancrer l'institution du «médecin-conseil» aussi dans le domaine de l'assurance privée.

La loi sur le contrat d´assurance (LCA), qui date de plus de cent ans, ne satisfait plus aux exigences actuelles. Une révision totale est censée l´adapter pleinement aux circonstances et aux besoins de notre temps. Dans le cadre de la consultation des offices, nous nous sommes exprimés sur certains points du projet touchant à la protection des données.

Beaucoup d´employeurs assurent leur obligation de continuer à verser le salaire à l´aide d´une assurance collective pour indemnités journalières en cas de maladie. Notamment dans les cas où les revenus à assurer sont élevés, les compagnies d´assurance demandent de passer un examen médical avant de signer le contrat. Cela peut avoir pour conséquence que certains employés ne sont pas acceptés ou seulement avec des réserves, ce qui conduit à un dilemme: l´employeur doit savoir dans quels cas l´assurance qu´il a contractée en vue de financer la continuation du versement du salaire ne paiera pas, étant donné qu´il devra alors lui-même prendre en charge ces prestations. Cela peut avoir des conséquences graves, particulièrement pour les petites entreprises. D´autre part, l´employé peut avoir un intérêt digne de protection à garder le secret sur ses problèmes de santé.

Le projet de consultation initial prévoyait de résoudre ce conflit d´intérêts en laissant l´employé décider s´il voulait communiquer un refus ou une admission sous réserves à son employeur. S´il devait craindre de perdre son emploi en révélant son état de santé, il devait avoir la possibilité de faire respecter la confidentialité. En contrepartie, l´obligation de l´employeur à continuer à payer le salaire serait dans ce cas limitée au montant minimum prévu dans le Code des obligations. Cette solution n´a cependant trouvé que peu d´approbation dans la procédure de consultation. Par conséquent, cette disposition a de nouveau été retirée du projet maintenant soumis au Parlement. Nous trouvons cela regrettable. La problématique décrite est du moins partiellement atténuée par le fait que la nouvelle législation sur l´assurance collective pour indemnités journalières en cas de maladie interdira de communiquer à l´employeur des informations sur l´état de santé ou la sphère intime de l´employé. Nous avons précisé dans notre prise de position que l´information transmise par la compagnie d´assurance à l´employeur après un examen médical doit se limiter à indiquer si l´employé est admis (le cas échéant avec des réserves) ou refusé. Cette précision a entretemps également été incluse dans le message.

Il est très réjouissant et important pour nous que notre intérêt, manifesté depuis longtemps à plusieurs reprises, d´ancrer l´institution du médecin-conseil dans le droit des assurances privées ait été pris en compte par le projet de révision. Pour l´instant, l´application obligatoire sera cependant limitée à l´assurance-maladie complémentaire et à l´assurance d´indemnités journalières. À notre avis, l´institution du médecin-conseil devrait à long terme faire l´objet d´une réglementation cohérente pour l´ensemble du droit des assurances privées et sociales.

1.6.2 Lutte contre la fraude à l'assurance dans le domaine des assurances-véhicules à moteur

Nos examens au sujet du «Car Claims Information Pool», une plateforme électronique de données des assureurs de véhicules à moteur, sont terminés. Les propositions d'amélioration de la protection et de la sécurité des données ont été acceptées.

L´échange électronique de données par l´intermédiaire du «Car Claims Information Pool» (CC-Info) permet aux assureurs suisses de véhicules à moteur de lutter contre la fraude à l´assurance. Ainsi, il doit permettre par exemple de découvrir les cas où un sinistre sur un véhicule est déclaré une deuxième fois auprès d´un autre assureur.

Nous avons, durant l'année sous revue, terminé nos recherches concernant CC-Info (cf. notre 18e rapport d'activités 2010/2011, ch. 1.6.1.) et soumis quelques propositions afin d'améliorer la protection et la sécurité des données: ainsi, CC-Info acceptait jusqu'ici plusieurs connexions simultanées avec le même identifiant, ce qui augmentait le risque que des personnes non autorisées accèdent au système. Le processus de connexion a été désormais adapté de manière à ne plus permettre une (nouvelle) connexion lorsqu'un utilisateur est déjà connecté au système avec le même identifiant. Nous avons également pu obtenir des améliorations concernant le traitement futur des demandes d'accès. Il existe désormais des directives claires à ce sujet.

Les personnes impliquées dans l'examen des faits ont, de manière appropriée à la situation, fait preuve de sensibilité aux questions de protection des données. Nous sommes convaincus que nos propositions d'amélioration contribueront de manière judicieuse à augmenter encore le niveau de protection des données, sans pour autant entraver de façon disproportionnée la fonctionnalité et la praticabilité du système.

1.6.3 Entraide administrative fournie aux autorités fiscales cantonales par l'assurance-accidents

Dans le cadre d'un avis de droit concernant l'art. 97 de la loi sur l'assurance-accidents, nous sommes arrivés à la conclusion que ce dernier règle de manière exhaustive les cas dans lesquels un assureur-accidents obligatoire doit communiquer des données aux autorités fiscales cantonales, en dérogation au devoir légal de discrétion.

Un assureur-accidents obligatoire nous a priés de rendre un avis juridique sur la question de savoir si les assureurs sont toujours tenus de fournir l'entraide administrative aux autorités fiscales cantonales conformément à l'art. 112, al. 2, de la loi fédérale sur l'impôt fédéral direct (LIFD) ou si l'obligation de renseigner se limite aux cas cités à l'art. 97 de la loi fédérale sur l'assurance-accidents (LAA). Nous sommes parvenus à la conclusion suivante:

Les assureurs-accidents obligatoires sont considérés comme des organes de la Confédération. Ils sont par conséquent soumis à la loi sur la protection des données (LPD). De ce fait, ils ne sont habilités à traiter et à communiquer des données que s'il existe une base légale pour ce faire. De plus, ils peuvent traiter et communiquer des données sensibles et des profils de la personnalité uniquement si une loi au sens formel le prévoit expressément.

Dans l'exercice de leurs tâches en matière d'assurance-accidents obligatoire, les assureurs traitent régulièrement des données personnelles sensibles. Le traitement de ces données nécessite donc une base légale au sens formel qui régit de manière expresse la manière dont les données peuvent être traitées, le genre de données qui peuvent être transmises et à qui. La communication de données sensibles aux autorités fiscales par les assureurs-accidents obligatoires doit être réglementée dans une loi fédérale. Un organe de la Confédération soumis au devoir légal de discrétion doit refuser la communication de données, la restreindre ou l'assortir de charges conformément à l'art. 19, al. 4, let. bLPD.

En principe, un assureur-accidents obligatoire est tenu de fournir les renseignements demandés aux autorités fiscales, en vertu des art. 112, al. 2, et 112a LIFD. Cette obligation générale de fournir des renseignements est toutefois en contradiction avec l'obligation de garder le secret prévue par l'art. 33 de la loi fédérale sur la partie générale du droit des assurances sociales (LPGA), qui est aussi applicable aux assureurs-accidents obligatoires. On ne peut y déroger que si une base légale le prévoit dans la LPGA elle-même ou dans une loi autonome.

Les exceptions au devoir de discrétion dans le domaine d'application de l'assurance-accidents obligatoire figurent à l'art. 97 LAA. Cette disposition établit dans les détails les cas dans lesquels l'assureur-accidents est habilité à communiquer des données à des tiers, en dérogation à l'art. 33 LPGA. L'art. 97 LAA renferme à l'al. 1, let. c, et à l'al. 2, une règle explicite sur la communication de données aux autorités fiscales, en rapport avec l'impôt à la source et l'impôt anticipé. Tous les autres cas sont soumis à la communication de données conformément à l'art. 97, al. 6, LAA.

Contrairement à d'autres lois sur les assurances sociales (par ex. l'art. 50a, al. 1, let. e, de la loi sur l'AVS ou l'art. 86a, al. 1, let. e, de la loi fédérale sur la prévoyance professionnelle vieillesse, survivants et invalidité), la LAA ne contient, s'agissant des communications de données aux autorités fiscales, aucune réglementation dans des cas d'espèce et sur demande écrite et motivée. Les tribunaux compétents devraient encore clarifier s'il s'agit ici d'un oubli du législateur ou d'une omission délibérée.

Nous sommes donc parvenus, sur la base de la législation actuelle, à la conclusion que l'art. 97 LAA règle de manière exhaustive les cas dans lesquels on peut déroger à l'obligation légale de garder le secret conformément à l'art. 33 LPGA et un assureur-accidents obligatoire doit communiquer les données demandées aux autorités fiscales. Les art. 112 et 112a LIFD ne sont donc pas applicables; en effet, leur application reviendrait à vider de sa substance la réglementation spéciale de l'art. 97 LAA.

Si une base légale manque, les organes de la Confédération peuvent exceptionnellement communiquer des données personnelles en se fondant sur l'art. 19, al. 1, let. a à d, LPD. Ces exceptions ne sont toutefois valables que dans des cas précis, énumérés exhaustivement à l'art. 19 LPD et qu'il convient d'interpréter de manière restrictive. Conformément à ces dispositions, un assureur-accidents obligatoire pourrait exceptionnellement transmettre les données nécessaires aux autorités fiscales cantonales.

1.7 Secteur du travail

1.7.1 Questions du public concernant la surveillance sur le lieu de travail

Les nombreux appels que reçoit notre service de consultation téléphonique sur le thème de la surveillance sur le lieu de travail le montrent: ni les employeurs, ni les employés ne sont au clair sur ce qui est véritablement autorisé.

De nombreux employeurs et employés ont contacté notre service de consultation téléphonique au cours de l'année écoulée pour se renseigner sur l'admissibilité de la surveillance sur le lieu de travail. Les thèmes les plus souvent cités ont été la vidéosurveillance, la surveillance des déplacements par le biais des téléphones intelligents (smartphones) de l'entreprise ou d'autres appareils, ainsi que la surveillance d'Internet et du courrier électronique.

En ce qui concerne les employeurs, nous avons constaté que leurs questions portaient principalement sur les procédés conformes à la protection des données. Quant aux employés, nous avons remarqué que la surveillance sur le lieu de travail n'était pas fondamentalement remise en question; la plupart sont conscients d'être surveillés et cette surveillance est également acceptée. Leurs questions ont plutôt porté sur ce que l'employeur a véritablement le droit de faire. Souvent, les personnes qui nous ont demandé conseil ont subi les critiques de leur employeurs à propos de leur comportement, ils faisaient l'objet d'une enquête en cours ou même avaient été congédiés.

Le problème fondamental, mais aussi la solution, c'est la garantie de la transparence, la clarté de la communication. L'employeur doit notifier précisément à ses employés la manière dont la surveillance est exercée et dans quel but elle est menée. Il doit donc les informer expressément, dans un règlement d'utilisation et de surveillance, des traitements de données qu'il effectue. De même, il doit indiquer clairement les utilisations du courrier électronique et d'Internet qui sont autorisées et celles qui sont interdites.

Bien entendu, la question de la proportionnalité des mesures de surveillance par rapport au but poursuivi se pose régulièrement dans ce domaine. À ce propos, nous devons dire que les possibilités techniques incitent certains employeurs à des actes de surveillance disproportionnés. Nous tenons donc à préciser clairement: une analyse nominative des données recueillies par le biais de l'utilisation de moyens d'information et de communication (téléphone, courrier électronique, Internet, fax) n'est autorisée qu'en présence d'un soupçon concret d'abus important. En outre, il est établi que le soupçon d'abus ne peut être clarifié par un autre procédé portant moins fortement

atteinte aux droits de la personnalité de l'employé. Enfin, il est interdit d'utiliser des systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail (art. 26 de l'ordonnance 3 relative à la loi sur le travail).

1.7.2 Remise de certificats des caisses de pension – Jugement du Tribunal administratif fédéral

Presque deux ans après que nous ayons demandé au Département fédéral de l'intérieur (DFI) d'empêcher la pratique, à notre avis illicite, de la remise des certificats des caisses de pension par l'intermédiaire de l'employeur (cf. notre 17e rapport d'activités 2009/2010, ch. 1.7.8 ainsi que notre 18e rapport d'activités 2010/2011, ch. 1.7.3), le département a pris une décision dans cette affaire. Nous n'étions pas d'accord avec la teneur de cette dernière et avons donc demandé au Tribunal administratif fédéral (TAF) d'ordonner à la caisse de pension d'envoyer à l'avenir les certificats personnels de manière telle que seules les personnes assurées, mais pas leur employeur, puissent prendre connaissance de leur contenu.

Dans son arrêt du 10 avril 2012 (A-4467/2011) le TAF a entièrement suivi notre argumentation. Il a retenu que la remise de certificats personnels par l'intermédiaire des employeurs, sous pli ouvert et non protégé, ne bénéficiait d'aucune base légale. Il a dès lors conclu que la caisse de pension avait violé son devoir de discrétion et le principe de la sécurité des données, et que les assurés concernés avaient ainsi subi une atteinte illicite à la personnalité.

L'arrêt du TAF n'était pas encore entré en force de chose jugée à la clôture de la rédaction.

1.7.3 Dossiers personnels électroniques dans l'administration fédérale

La révision de la loi sur le personnel de la Confédération a permis de créer la base légale nécessaire au système électronique d'information sur le personnel ainsi qu'aux dossiers électroniques du personnel et aux dossiers électroniques de candidature.

Dans le secteur privé, les dossiers électroniques du personnel et les dossiers électroniques de candidature sont courants. Mais les organes de la Confédération sont tenus de respecter le principe de légalité, selon lequel tout traitement de données nécessite une base légale. Pour ce qui est du traitement de données sensibles et de profils de la personnalité, cette base légale doit en outre se trouver dans une loi fédérale au sens formel. Les dossiers personnels et les dossiers de candidature contiennent selon toute

probabilité des données personnelles sensibles et constituent en général un profil de la personnalité. En l'absence d'autorisation prévue par une loi fédérale au sens formel, il n'aurait donc pas fallu gérer jusqu'ici ni dossier électronique du personnel, ni dossier électronique de candidature au sein de l'administration fédérale. De même, le système d'information sur le personnel de l'Office fédéral du personnel (OFPER) n'était réglementé jusqu'à présent que par une ordonnance.

La modification de la loi fédérale sur le personnel de la Confédération (LPers, art. 27a à 27c) a permis de créer la base légale requise pour le système d'information concernant le personnel de la Confédération (BV PLUS), la gestion électronique des candidatures (postulations en ligne) et les dossiers personnels électroniques. Cette modification a en outre nécessité une révision de l'ordonnance concernant la protection des données personnelles dans l'administration fédérale. Les dispositions en question sont entrées en vigueur le 1er janvier 2012. Durant l'année écoulée, nous avons contribué de manière importante à l'élaboration de ces dispositions et apporté une collaboration soutenue à l'OFPER.

1.7.4 Contrôle du système d'information en matière de placement et de statistique du marché du travail

La documentation du système d'information en matière de placement et de statistique du marché du travail PLASTA a été améliorée. Des divergences demeurent néanmoins entre ce qui devrait exister dans un règlement et ce qui s'y trouve réellement. Il convient notamment d'améliorer la documentation des processus dans le règlement de traitement, de même la règlementation des droits d'accès et du chiffrement.

Lors de notre contrôle nous avons constaté que certains domaines avaient fait l´objet d´améliorations. Il subsiste néanmoins quelques points importants qui doivent être mieux documentés. Nous avons entre autres attiré l´attention sur le fait que les processus, depuis la collecte des données personnelles jusqu´à leur anonymisation ou destruction, doivent être documentés. En particulier, les processus qui traitent des données sensibles ou des profils de la personnalité doivent être documentés dans le règlement de traitement. Ainsi il est possible de retrouver quelles données ont été traitées, où, par quels moyens, par quels organes ou unités organisationnelles et à quelles fins. La documentation actuelle des processus tient sur une seule page A4 du règlement et est trop limitée. Elle devrait contenir un résumé significatif plutôt que de multiples références à des informations plus détaillées contenues dans d´autres documents.

Nous avons également constaté que la réglementation des accès aux données n´est pas assez restrictive. En l´état actuel de nos connaissances, tous les utilisateurs du

système dans le canton peuvent effectuer une recherche selon le nom, prénom, l´identificateur de personne ou le numéro AVS. À notre avis, la recherche avec l´un des deux numéros est conforme à la protection des données parce qu´elle affiche directement la bonne personne. La recherche selon le nom ou le prénom fournit par contre trop de résultats. Une telle recherche ne devrait être possible que si l´on est en mesure de saisir le nom et le prénom ainsi qu´une indication supplémentaire. Ceci pourrait bien sûr être la date de naissance. Cette dernière n´est cependant pas idéale, car cette information est connue dans de nombreux cas et permettrait ensuite des interrogations à des fins contraires. Il serait important de saisir, en plus du nom et du prénom, une donnée que la personne concernée connaît par cœur mais qu´un tiers ne découvrirait pas aisément. On pourrait envisager, pour des cas exceptionnels, de permettre la recherche selon le nom uniquement. Ces requêtes devraient cependant être journalisées de manière conforme aux exigences de la révision. Nous avons en outre relevé que les données personnelles sensibles doivent également être cryptées dans les supports de stockage. Cette exigence est le plus souvent rejetée avec l'argument selon lequel cela entraverait fortement les performances du système. Nous avons donc demandé aux responsables de PLASTA de nous fournir des informations détaillées à ce sujet.

1.8 Économie et commerce

1.8.1 La protection des données face à l'informatique en nuage

De plus en plus d'entreprises, d'autorités et d'institutions confient le traitement de leurs données à des entreprises externes, misant sur l'informatique en nuage. Ce mode de traitement offre certes de nombreux avantages, mais en parallèle, il ne faut pas en négliger les risques techniques et juridiques au regard du droit de la protection des données. Nous avons donc publié des commentaires explicatifs concernant l'informatique en nuage. Ils en soulignent les risques et présentent les impératifs qui y sont attachés.

Certes la protection des données revient régulièrement dans les conversations lorsqu'il s'agit d'externalisation (outsourcing) et d'informatique en nuage (cloud computing), mais elle est régulièrement confondue avec la sécurité des données. Cette dernière est indubitablement un élément extrêmement important, mais la protection des données face à l'informatique en nuage est bien plus importante. Dans bien des cas justement, le transfert de traitements de données vers un «nuage public» étranger ne peut tenir compte des exigences du droit de la protection des données sous tous ses aspects. D'une part, souvent, les prestataires de l'informatique en nuage n'indiquent pas de manière claire où les données sont traitées. D'autre part, le traitement des données est fréquemment effectué dans un pays qui ne dispose pas d'une législation suffisante sur la protection des données.

Avant de mettre des données dans un nuage, il faut choisir soigneusement le prestataire en procédant à une analyse des risques; il faut aussi lui donner des instructions précises et le surveiller attentivement. La transparence du prestataire sur le traitement des données et la garantie de la sécurité des données sont des critères de choix importants. Une règle générale: plus les données sont confidentielles, secrètes, importantes (parce que d'un enjeu décisif pour l'entreprise) ou sensibles (parce que particulièrement dignes de protection), plus leur délocalisation dans un nuage, en particulier à l'étranger, est à déconseiller et plus les mesures de sécurité et de contrôle (en matière de protection des données) doivent être strictes et complètes. Car au bout du compte, c'est l'utilisateur du service en tant que mandataire qui demeure responsable du respect des prescriptions en matière de protection des données vis-à-vis des personnes concernées et c'est lui qui répond des éventuelles atteintes à la personnalité.

Ces explications concernant l'informatique en nuage sont aussi disponibles en français sur le site Internet du préposé fédéral à la protection des données www.leprepose.ch sous la rubrique Thèmes – Protection des données – Entreprises.

1.8.2 Traitement de données par des sociétés de renseignements commerciaux, économiques et sur la solvabilité

Nous observons depuis longtemps que les sociétés de renseignements commerciaux, économiques et sur la solvabilité ont tendance à traiter de plus en plus de données concernant des personnes. Cette année, nous avons mené auprès d'une grande agence un examen complet des faits et vérifié leurs traitements de données quant à la conformité avec la loi sur la protection des données. Le traitement des données de personnes physiques et de personnes morales dans le but d'évaluer leur solvabilité était au cœur de nos préoccupations.

Comme nous l'avons déjà mentionné dans de précédents rapports d'activités, nous sommes chaque année confrontés à de nombreuses questions de citoyens à propos du traitement de données mené par des agences d'évaluation du crédit et des agences de renseignement économique. En outre, nous observons également depuis longtemps que les agences de renseignement économique traitent de plus en plus de données sur des personnes et utilisent aussi des informations d'ordre sociodémographique en donnant comme argument qu'elles ont besoin de ces données pour vérifier la solvabilité des personnes concernées. En font partie entre autres des informations sur l'endroit où une personne habite ou encore pour quelle somme elle aurait acheté, construit ou rénové une maison ou un appartement. Ces données sont ensuite reliées à Google Street View. Nous considérons que cette mise en relation n'est pas conforme aux dispositions en matière de protection des données.

Au cours de l'année sous revue, nous avons mené auprès d'une grande agence d'évaluation du crédit et de renseignement économique un examen complet des faits concernant le traitement des données de personnes physiques et de personnes morales dans le but d'évaluer leur solvabilité. Nous avons particulièrement concentrés nos recherches sur les aspects suivants: quelles sont les données actuellement nécessaires afin d'identifier sans ambigüité une personne; quelles sont les informations qui constituent la base de l'examen de sa solvabilité; d'où proviennent ces informations, combien de temps elles demeurent stockées et à partir de quelles informations l'on établit, le cas échéant, une notation de la solvabilité. Nous avons en outre examiné ce qu'il en était de la transparence et de l'identification des sources des données, du contenu des données et du calcul de la solvabilité et comment les demandes de

renseignement, de rectification ou d'effacement sont traitées. De plus, nous avons clarifié quelles données l'agence transmet à des tiers dans le cadre de l'examen de la solvabilité et vérifié s'il est garanti que cela n'a lieu que pour conclure ou exécuter un contrat avec la personne concernée. Enfin, nous avons examiné si l'ensemble des données traitées constitue un profil de la personnalité.

Nous avons constaté avec satisfaction qu'à de nombreux égards, le traitement des données était conforme aux prescriptions en matière de protection des données. En outre, nous avons pu trouver, avec l'agence en question, des solutions conformes au droit de la protection des données à propos des points visés par nos critiques. Cette agence s'est montrée très coopérative et très constructive durant tout le temps de nos recherches. L'examen des faits a été mené à terme avec succès.

1.8.3 Traitement de données personnelles par un fournisseur de services de télécommunication

Une question qui revient régulièrement est celle de savoir dans quelle mesure les collaborateurs d'un service de télécommunication ont accès aux données clients. Certains collaborateurs ont besoin dans le cadre de leur travail d'accéder à de telles données. Toutefois, l'accès à ces données dans un but privé est un abus que l'on doit empêcher par la mise en place de mesures techniques et organisationnelles.

Une personne nous a signalé que certains collaborateurs d'un fournisseur de services de télécommunication avaient un accès illimité à des données de clients, y compris les données secondaires et surtout les contenus de SMS, et les utilisaient à des fins privées. Nous avons procédé à un examen des faits et constaté que les mesures prises par le fournisseur de services de télécommunication afin d'empêcher les accès abusifs à ces données étaient proportionnées au but visé.

Parmi les mesures organisationnelles, mentionnons la nécessité de formuler une demande formelle pour les autorisations d'accès, de les octroyer selon le principe dit du privilège minimal (accès strictement limité aux informations absolument nécessaires) et de mettre en œuvre des concepts de sécurité, ainsi que le devoir de confidentialité des collaborateurs, leur sensibilisation et leur formation. Sur le plan technique, les accès font l'objet d'une journalisation et d'une analyse en cas de soupçon. Les risques d'abus sont ainsi ramenés à un niveau acceptable grâce à l'association des mesures techniques et organisationnelles.

Pour ce qui est de l'accès aux SMS, nous avons constaté que ceux-ci ne sont stockés dans le système du fournisseur de service que lorsque le destinataire n'est pas atteignable. Dès que le message entreposé est remis, il est automatiquement effacé de la centrale des SMS. Si le destinataire ne peut être atteint dans le délai d'une semaine, le message est automatiquement effacé. Ainsi, grâce à ce type de traitement des communications, à la politique d'autorisation fondée sur le principe du privilège minimal, ainsi qu'à d'autres mesures techniques, il est permis d'exclure presque entièrement un accès illicite aux contenus des messages par les collaborateurs.

1.8.4 Nouvelle ordonnance de la FINMA sur les données

Les plus hauts organes d'un institut contrôlé par la FINMA doivent offrir la «garantie d'une activité irréprochable». Ce «contrôle de garantie» est du ressort de la FINMA qui gère à cet effet un fichier dont les détails sont réglementés par la nouvelle ordonnance de la FINMA sur les données.

Les lois sur les marchés financiers requièrent que les organes les plus élevés d'un institut contrôlé par l'Autorité fédérale de surveillance des marchés financiers (la FINMA) offrent «la garantie d'une activité irréprochable». Pour ces instituts, cette «condition de garantie» est une condition d'autorisation qu'il convient de respecter en tout temps. «L´examen de la garantie» incombe à la FINMA. À cet effet, elle saisit dans un fichier les données des personnes ne présentant pas toutes les garanties d'une activité irréprochable conformément aux lois sur les marchés financiers ainsi que celles dont une telle garantie doit être contrôlée. La loi sur l'Autorité fédérale de surveillance des marchés financiers (loi sur la surveillance des marchés financiers, LFINMA) constitue la base légale du traitement de ces données et habilite la FINMA à en régler les détails. Si ce type de réglementation manquait jusqu'ici, l'entrée en vigueur de la nouvelle ordonnance de la FINMA sur les données au 1er octobre 2011 a permis de combler cette lacune. Étant donné que la FINMA traite dans le cadre de «l'examen de la garantie» des données particulièrement sensibles et des profils de la personnalité, nous avons examiné cette nouvelle ordonnance, notamment sous l'angle du traitement de ce genre de données, et soumis à la FINMA des suggestions en la matière dont la majeure partie ont été mises en œuvre.

1.8.5 Traitement de données personnelles dans le secteur de la vente d'adresses

Nous avons procédé à un examen des faits auprès d'un commerçant d'adresses. Nous avons cependant constaté que les exigences de la protection des données n'étaient pas toujours remplies, et en particulier que les personnes exerçant leur droit d'accès ne recevaient pas la totalité des informations enregistrées à leur sujet. La transparence, notamment quant à l'origine des données collectées, doit aussi être améliorée.

Nous avons procédé à un examen des faits auprès d'un commerçant d'adresses et examiné si les traitements de données effectués étaient conformes aux prescriptions de la loi fédérale sur la protection des données (LPD) (cf. ch. 1.8.4 de notre 18e rapport d'activités 2010/2011). Dans l'ensemble, les examens ont montré que le commerçant d'adresses concerné s'efforce de traiter les données de manière conforme aux exigences de la protection des données. Néanmoins, nous avons constaté qu'il ne répond pas aux exigences de la LPD dans certains domaines et que des améliorations sont donc nécessaires.

En résumé, on peut relever que la transparence de la collecte et du traitement des données est insuffisante pour les personnes concernées. Des améliorations s'imposent donc. La droit d'accès représente à cet effet un instrument essentiel pour les personnes concernées. Le commerçant d'adresses doit, sur demande, communiquer au requérant toutes les données qui le concernent, y compris toutes les indications disponibles sur leur origine. C'est ainsi seulement qu'une personne peut constater quelles données sont traitées à son sujet et décider si elle a intérêt à faire valoir d'autres droits relatifs à la protection des données (en particulier le droit d'opposition).

Nous avons également souligné que l'utilisation à des fins de marketing des données publiées dans l'annuaire constitue une atteinte à la personnalité lorsque la personne concernée a fait apposer un astérisque auprès de son inscription. Seul un consentement peut en principe justifier une telle utilisation (cf. ch. 1.8.6 du présent rapport d'activités).

Enfin, il convient de noter que les données qui ont été collectées à des fins publicitaires ne peuvent en principe pas être utilisées à d'autres fins. Au cas où celles-ci sont communiquées à des tiers, le commerçant d'adresses doit prendre les mesures nécessaires pour que cette finalité soit respectée.

Les examens étaient encore en cours au moment de la rédaction du présent rapport d'activités.

1.8.6 Utilisation de l'adresse publiée dans l'annuaire à des fins de marketing

Nous sommes d'avis que par l'apposition de l'astérisque dans l'annuaire téléphonique, l'abonné indique qu'il s'oppose à toute utilisation de ses données d'annuaire à des fins publicitaires, donc non seulement au télémarketing mais également à la publicité adressée. Or cette position s'oppose à la pratique actuelle de nombreux professionnels de la publicité, qui collectent et utilisent les adresses figurant dans l'annuaire avec la mention d'un astérisque à des fins de prospection publicitaire.

Par l'apposition de l'astérisque dans l´annuaire téléphonique, l'abonné déclare qu'il s'oppose de façon générale à toute utilisation de ses données d'annuaire à des fins publicitaires, ce qui comprend à notre avis non seulement le télémarketing mais également la publicité adressée par voie postale. Inversément, l'absence d'astérisque signifie que l'abonné ne s'oppose pas à l'utilisation de ces données à des fins de marketing direct et que celles-ci peuvent donc être en principe utilisées dans ce contexte. Cela étant, la personne concernée a toujours la possibilité de s'opposer au cas par cas au traitement de ses données personnelles (voir à ce sujet notre publication sur notre site web www.leprepose.ch – Documentation – Protection des données – Feuillets thématiques – Blocage de l'utilisation d'une adresse à des fins publicitaires).

Au cours de l'examen des faits auprès d'un commerçant d'adresses (cf. ch. 1.8.5), nous avons constaté que celui-ci collectait toutes les données figurant dans l'annuaire téléphonique – y compris les inscriptions dotées d'un astérisque – et les communiquait à des tiers à des fins de marketing. Selon le commerçant d'adresses en question, l'astérisque ne se rapporterait qu'au numéro de téléphone et aux autres données utilisées à des fins de télécommunication, mais non à l'adresse postale. De son point de vue, les données d'annuaire peuvent sans autre être utilisées pour envoyer de la publicité adressée, même lorsque l'astérisque figure auprès des inscriptions.

Nous apprécions la situation juridique comme suit. L'art. 88 de l'Ordonnance sur les services de télécommunication (OST) est formulée de façon très générale: «Les clients figurant dans un annuaire ont le droit d'y faire mentionner clairement qu'ils ne souhaitent pas recevoir de messages publicitaires de tiers et que les données les concernant ne peuvent pas être communiquées à des fins de prospection publicitaire directe». Par ailleurs, depuis le 1er avril 2012, le non respect de l'astérisque dans l'annuaire est également considéré comme un acte déloyal au sens de l'art. 3 lit. u de la loi fédérale sur la concurrence déloyale (LCD) et peut être sanctionné sur le plan pénal. Même si l'on devait considérer que ces dispositions légales ne s'appliquent que dans le domaine des télécommunications (à savoir pour le télémarketing), cela ne signifie pas pour autant

que l'utilisation, à des fins de marketing, de l'adresse figurant dans l'annuaire soit licite. En effet, sous l'angle de la législation sur la protection des données (LPD), toute collecte de données et en particulier sa finalité doit être reconnaissable pour la personne concernée et toute communication de données doit respecter les principes de finalité et de transparence. Or, une utilisation des données publiées dans l'annuaire à des fins de prospection publicitaire n'est pas reconnaissable pour la personne concernée qui a fait apposer un astérisque auprès de son inscription; une telle utilisation des données représente également une violation du principe de finalité, l'annuaire ayant avant tout pour but de permettre l'établissement des télécommunications (et non l'envoi de publicité) et la publication obligatoire de l'adresse postale visant à identifier de façon certaine l'abonné à des fins de télécommunications.

C'est pourquoi nous estimons que l'utilisation, à des fins de marketing, des adresses publiées dans l'annuaire constitue une atteinte illicite à la personnalité, à moins d'être justifiée dans un cas concret par le consentement de la personne concernée (p. ex. concours ou relation commerciale).

1.9 Finances

1.9.1 Communication de données à des autorités fiscales étrangères

La communication de données aux autorités fiscales étrangères demeure une des priorités de l'agenda politique et ce thème suscite un vif débat auprès du public. Du point de vue de la protection des données, nous avons tout particulièrement porté notre attention sur les conventions de double imposition, sur la nouvelle loi fédérale sur l'assistance administrative en matière fiscale, ainsi que sur le Foreign Account Tax Compliance Act, le FATCA.

Conventions de double imposition

Comme il l'a déjà fait à plusieurs reprises, le Conseil fédéral continue à conclure de nouvelles conventions visant à éviter la double imposition (CDI) ou en révise dans la perspective de la mise sur pied d'une entraide administrative internationale en matière fiscale et dans l'optique de la reprise des normes de l'OCDE (notamment en ce qui concerne l'échange d'informations). Nous nous sommes déjà exprimés sur ce sujet (voir notre 18e rapport d'activités 2010/2011, ch. 1.9.3). Le 13 février 2011, le Conseil fédéral a décidé d'adapter les conditions relatives à l'identification des contribuables et des détenteurs de renseignements aux normes de l'OCDE applicables au niveau international. Désormais, il pourra être donné suite à une demande d'assistance administrative qui repose sur une CDI comportant une disposition relative à l'échange d'informations conformément à l'art. 26 du modèle de convention de double imposition de l'OCDE lorsqu'il y est démontré qu'il ne s'agit pas d'une «fishing expedition» et (a) lorsque l'Etat requérant identifie le contribuable, cette identification pouvant aussi avoir lieu d'une autre manière que par l'indication du nom et de l'adresse, dans certains cas exceptionnels même par l'indication d'un numéro de compte; ou (b) lorsque l'Etat requérant donne le nom et l'adresse du détenteur présumé des informations dans la mesure où ils lui sont connus. Si ces indications qui permettraient à la Suisse d'identifier le détenteur des informations manquent, il faut respecter les principes de la proportionnalité et de la praticabilité. Les demandes accompagnées d'une liste de numéros de comptes sans aucune autre indication serait considérée comme une pêche aux informations à laquelle il ne serait pas donné suite. Sur la base de ces éléments, nous sommes parvenus à la conclusion que cette pratique est conforme à la protection de données.

Loi sur l'assistance administrative en matière fiscale

Les clauses d'assistance administrative dans les conventions de double imposition et autres conventions internationales en matière fiscale ne règlent pas ce qu'il convient de faire à ce propos au niveau national. Actuellement, cette question est régie par l'ordonnance relative à l'assistance administrative d'après les conventions contre les doubles impositions (OACDI); toutefois, cette ordonnance ne satisfait pas aux exigences du principe de légalité. Pour cette raison, le Conseil fédéral a élaboré un projet de loi fédérale sur l'assistance administrative internationale en matière fiscale (loi sur l'assistance administrative fiscale, LAAF). Cette loi prévoit que l'assistance administrative doit se dérouler dans le cadre des conventions mentionnées, lesquelles prévoient un échange d'informations en matière fiscale.

En principe, la loi sur la protection des données est aussi applicable à l'assistance administrative internationale en l'absence de loi spéciale. Toutefois, dans le cas de l'assistance administrative en matière fiscale, la LAAF primera désormais en tant que lex specialis sur la loi sur la protection des données. Dans le cadre de la consultation des offices, nous avons examiné le projet de loi sous l'angle de sa compatibilité avec la loi sur la protection des données (LPD) et sommes parvenus à la conclusion que les exigences prévues par le droit de la protection des données sont remplies pour ce qui est du principe de légalité (art. 17 LPD) et de la communication de données personnelles à des tiers (art. 19 LPD). Le but du traitement, les indications sur la personne qui traite les données et leur destinataire, ainsi que le volume des données acquises, de leur traitement et de leur communication y sont réglementées en détail et les droits des personnes concernées sont garantis.

Foreign Account Tax Compliance Act (FATCA)

Le «Foreign Account Tax Compliance Act» (FATCA) est une loi des États-Unis d'Amérique qui entrera en vigueur le 1er janvier 2013. Elle vise à contrer l'évasion fiscale des contribuables américains. Tous les instituts financiers étrangers («Foreign Financial Institutes» FFI) sont concernés par ces nouvelles dispositions légales; il s'agit des banques et des assurances entre autres qui investissent pour leurs clients ou pour leur propre compte dans des titres américains. Ceux-ci seront tenus, annuellement, de fournir automatiquement des informations complètes sur les contribuables américains aux autorités fiscales des États-Unis («Internal Revenue Service IRS»), faute de quoi elles seront tenues de s'acquitter d'un impôt à la source de 30% («withholding tax») sur tous les paiements de revenus de provenance étasunienne. Sont considérés comme contribuables américains les ressortissants américains, les doubles nationaux, les détenteurs d'une green card, mais aussi les personnes qui fiscalement possèdent le statut de résident. Il faudra donc communiquer aux autorités fiscales des États-Unis

pour chaque titulaire de compte le nom, l'adresse, le TIN (tax identification number), le numéro de compte, le solde, les revenus bruts et les retraits bruts ou autres transactions. Si un compte soumis à déclaration est identifié, son titulaire ou l'ayant droit économique doit donner son consentement à la communication des données en question aux États-Unis; le secret bancaire est ainsi levé. Au cas où la personne refuse ce consentement, la relation bancaire doit être dissoute et l'information doit être transmise aux autorités fiscales américaines.

Nous sommes très critiques à l'égard de cette loi américaine imposée unilatéralement par les États-Unis. D'une part parce que la communication directe de données d'instituts financiers privés aux autorités fiscales américaines revient de facto à un échange automatique d'informations, en contournement de la voie usuelle de l'assistance administrative. D'autre part, nous sommes d'avis que le FACTA n'est pas conforme à notre loi sur la protection des données, et cela à divers égards. Dans le cadre d'une audition devant la Commission de politique étrangère du Conseil des États, nous avons eu la possibilité de faire part de nos préoccupations à ce sujet. Nos réserves portent notamment sur la validité du consentement à la levée du secret bancaire, à la proportionnalité quant aux personnes qui sont considérées comme contribuables américains ainsi qu'au volume et au contenu des données qui doivent être communiquées. Enfin, nous considérons comme problématique le fait que les autorités fiscales des États-Unis ne soient pas tenues par une obligation de confidentialité à l'égard des informations reçues.

1.9.2 Étude concernant la modernisation des poursuites en Suisse

L'étude de l'Office fédéral de la justice publiée en 2011 à propos de la norme de communication e-LP a porté sur la modernisation des poursuites en Suisse et a montré les chances et les risques d'un office des poursuites virtuel, doté d'un registre central des poursuites. L'introduction et l'utilisation d'un identificateur de personnes est la pierre angulaire de ce type de registre.

Nous avons été invités à nous prononcer sur l'étude e-LP dans la perspective d'une modernisation des poursuites en Suisse. Cette étude entendait souligner le potentiel d'un réseau e-LP et montrer les risques et les possibilités d'un office des poursuites virtuel en Suisse, doté d'un registre des poursuites central. Nous nous sommes tout particulièrement penchés sur deux thèmes, à savoir l'identificateur de personnes et la banque de données centrale des débiteurs.

L'identification sûre et sans équivoque des personnes est la pierre angulaire d'un office des poursuites virtuel doté d'un registre des poursuites central. À cette fin, l'office aurait besoin d'un identificateur de personnes. L'identification est plus facile pour les personnes morales que pour les personnes physiques, puisqu'on peut utiliser par exemple le numéro d'identification des entreprises (IDE). Il est d'ores et déjà possible d'obtenir ce numéro IDE en ligne car il se trouve dans un registre accessible au public. Il est par contre beaucoup plus difficile d'envisager la création d'un identificateur sans équivoque pour les personnes physiques. Nous trouvons au premier plan l'utilisation du numéro d'assurance sociale (NAVS13). Mais cette option implique de grands risques pour la sphère privée des citoyens car elle permettrait d'établir des liens indésirables. Mis à part le fait que conformément à la loi sur l'AVS, il faudrait d'abord créer la base légale nécessaire, nous estimons qu'une utilisation systématique du NAVS13 n'entre pas en ligne de compte dans un registre central des poursuites: le NAVS13 ne permet pas toujours d'identifier une personne sans équivoque; de plus, toutes les personnes physiques qui peuvent être mises aux poursuites n'ont pas un numéro d'AVS. Pour que l'utilisation du NAVS13 soit judicieuse, il faudrait aussi qu'un créancier potentiel qui veut introduire une poursuite ou un tiers qui demande un extrait du registre des poursuites concernant un débiteur puisse l'identifier sans équivoque. Il faudrait donc qu'ils connaissent son numéro d'AVS. Il s'en suivrait une diffusion massive des numéros d'AVS qui réduirait à néant la gestion restrictive de leur utilisation.

Une banque de données centrale des débiteurs qui viendrait remplacer le système actuel des registres décentralisés des poursuites offrirait de grands avantages. Elle permettrait par exemple d'éliminer la diversité (déjà maintes fois critiquée), tant du point de vue temporel que du contenu, des traitements effectués à partir des renseignements tirés des registres des offices des poursuites. Mais une banque de données centrale et électronique comporterait aussi des risques considérables. Les données devraient dans tous les cas être protégées contre la perte accidentelle et les erreurs techniques, mais aussi contre la falsification, le vol et autres traitements contraires au droit. Elles ne devraient pas être modifiées, copiées ou même détruites par des personnes non habilitées. En outre, dans un système décentralisé, la confidentialité, la disponibilité et l'intégrité de données aux origines les plus diverses devraient être aussi garanties en tout temps.

L"étude en question ayant dans un premier temps abordé les chances et les risques d'un office des poursuites virtuel en Suisse uniquement d'un point de vue général, il faut encore attendre de savoir quelle option, parmi les nombreuses possibilités abordées, sera effectivement mise en pratique. Nous continuerons à suivre le projet et si cela est nécessaire et utile, nous intégrerons nos points de vue dans le débat de manière constructive.

1.9.3 Révision de l'ordonnance régissant la taxe sur la valeur ajoutée

L'ordonnance régissant la taxe sur la valeur ajoutée ne constitue pas une base légale suffisante permettant l'utilisation du numéro d'AVS dans le domaine de la taxe sur la valeur ajoutée, même pas comme disposition transitoire.

Dans le cadre d'une consultation des offices, nous avons été invités à nous prononcer sur la révision de l'ordonnance régissant la taxe sur la valeur ajoutée (OTVA). Il s'agissait de modifier, dans le sens d'une disposition transitoire, l'art. 131, let. a, OTVA pour que le numéro AVS puisse également être utilisé dans le domaine de la taxe sur la valeur ajoutée. Cela bien que la loi sur l'AVS prescrive clairement que le numéro AVS ne peut être utilisé systématiquement en dehors des assurances sociales fédérales que si une loi fédérale le prévoit et si le but de l'utilisation et les utilisateurs légitimés sont définis. Selon la jurisprudence, il est possible de déroger à la règle qui exige une loi au sens formel et d'envisager une réglementation au niveau de l'ordonnance (en tant que disposition transitoire) lorsque l'élaboration de la base légale au sens formel est déjà concrètement en cours, sur le plan matériel et temporel. Cette règle a pour but d'éviter que suite à la création d'un précédent (à savoir la réglementation d'un objet au niveau de l'ordonnance au lieu de la loi) le législateur ne se voit ôter la possibilité de faire usage des compétences qui lui reviennent et d'édicter des lois qui répondent à sa volonté. Une disposition transitoire au niveau de l'ordonnance suffit par exemple si le projet de loi et le message qui l'accompagne sont établis et ont été discutés au moins dans l'une des chambres de l'Assemblée fédérale. Mais dans le cas présent, ces conditions n'étaient pas encore remplies, raison pour laquelle nous nous sommes prononcés contre la modification de l'art. 131, let. a, OTVA. L'office responsable a finalement renoncé à cette modification.

1.9.4 Obligation de renseigner des établissements cantonaux d'exécution des peines envers les offices des poursuites

Avant la notification du commandement de payer, les offices des poursuites doivent entreprendre toutes les recherches raisonnables et nécessaires afin de retrouver un débiteur. En font aussi partie les vérifications auprès des autorités cantonales d'exécution des peines à propos du séjour des personnes incarcérées. Ce type de vérifications peut être raisonnablement exigé des autorités.

Une autorité cantonale d'exécution des peines et un office des poursuites du même canton n'étaient pas d'accord sur la question de savoir si et dans quelle mesure une

autorité d'exécution des peines doit fournir à l'office des poursuites des renseignements sur le séjour de personnes dans une de leurs institutions, cela dans le but de notifier un commandement de payer. D'une manière générale, nous ne sommes pas compétents pour répondre à ce genre de question. Mais, dans le cas présent, comme il s'agissait de l'interprétation du droit fédéral, nous avons été priés de remettre une appréciation juridique.

Le droit de ce canton en matière de protection des données prévoyait qu'une autorité peut communiquer des données personnelles sensibles si l'action repose clairement sur une base légale, si la personne concernée y a consenti expressément ou encore si l'accomplissement d'une tâche légale le requiert absolument. Dans le cas présent, ni le droit cantonal, ni la loi fédérale sur la poursuite pour dettes et la faillite (LP) ne contiennent de règlementation dans ce sens et il n'y avait pas non plus de consentement de la personne concernée. La question se posait donc de savoir si l'autorité d'exécution des peines doit communiquer le lieu de séjour d'une personne incarcérée parce que cette communication est nécessaire à l'accomplissement d'une tâche légale de l'office des poursuites.

Si un débiteur a son domicile en Suisse, la notification du commandement de payer est régie par les art. 71 et 72 LP ainsi que par les prescriptions générales des art. 64 et suivants LP concernant la notification des actes de poursuite. Lorsque la poursuite est dirigée contre un détenu qui n'a pas de représentant, l'office des poursuites lui accorde un délai conformément à l'art. 60 LP pour en nommer un, à moins que de par la loi, ce soit à l'autorité tutélaire de le nommer. La poursuite demeure suspendue jusqu'à l'expiration de ce délai, lequel doit être accordé avant la notification du commandement de payer (ATF 77 III 145, cons. 1). Conformément à la jurisprudence du Tribunal fédéral, l'art. 60 LP a pour but de permettre au représentant (légal) d'un détenu d'accomplir les actes nécessaires en procédure de poursuite (cf. ATF 38 I 237, ainsi que 108 III 3, cons. 1). Le débiteur doit être à même de pouvoir se défendre de manière efficace contre des actes de poursuite illégaux ou inadaptés. L'inobservation de l'art. 60 LP dans le cas de la notification d'un commandement de payer a pour conséquence l'invalidation de la mesure de l'office des poursuites et une notification erronée du commandement de payer (c'est-à-dire qui ne parvient pas à la connaissance du débiteur) est nulle (ATF 120 III 117, cons. 2c).

Si l'office des poursuites doit fixer un délai au détenu ou à son représentant avant la notification du commandement de payer conformément à l'art. 60 LP, cela suppose qu'il a connaissance du fait que cette personne est en détention ou en train d'exécuter une peine. De ce fait se pose inévitablement la question de savoir comment l'office

des poursuites parvient à cette information ou quand et jusqu'à quel point il doit procéder à des recherches sur le lieu de domicile ou de séjour d'un débiteur avant de notifier le commandement de payer.

Avant que l'office entreprenne des recherches sur le lieu de domicile ou de séjour, il a la possibilité de notifier le commandement de payer conformément à l'art. 64 et l'art. 66, al. 1 et 2, LP, à savoir au lieu de domicile, au lieu de la formation professionnelle, dans un local désigné par le débiteur ou par l'intermédiaire de la poste. Dans toutes ces formes de notification, il doit être garanti que le débiteur est véritablement informé du commandement de payer, faute de quoi la poursuite est nulle. Si le commandement de payer ne peut être notifié par cette voie, la notification peut se faire par publication officielle (notification par voie édictale, art. 66, al. 4, LP). De l'avis du Tribunal fédéral, ce mode de notification est un ultime moyen; il ne faut pas y recourir avant que toutes les recherches basées sur la situation de fait aient été entreprises par le créancier et l'office des poursuites pour découvrir une éventuelle adresse de notification du débiteur (ATF 112 III 6, cons. 4). Il ne doit pas y avoir de notification édictale dès que l'on estime que les données constituant l'adresse ne suffisent pas, mais seulement lorsque le débiteur demeure inatteignable ou lorsque les recherches semblent sans espoir. On peut en conclure que dans certains cas d'espèce où une notification conformément aux art. 64 et 66, al. 1 et 2, LP est impossible et où l'on ne dispose d'aucun indice sur l'endroit où se trouve le débiteur, un office des poursuites doit demander aux autorités d'exécution des peines et aux établissements pénitentiaires si un débiteur se trouve éventuellement en détention ou est en train d'exécuter une peine. Cela ne signifie toutefois pas qu'un office des poursuites doit adresser sa demande auprès des autorités d'exécution des peines des 26 cantons. Cela ne serait ni faisable, ni raisonnablement exigible. Par contre, s'adresser aux autorités d'exécution des peines de son propre canton semble une démarche raisonnable.

Nous sommes donc parvenus à la conclusion suivante: les offices des poursuites doivent impérativement respecter l'art. 60 LP et déjà avant la notification d'un commandement de payer, entreprendre toutes les recherches nécessaires et raisonnablement exigibles pour trouver un débiteur. Par ailleurs, ils ont absolument besoin de l'information requise auprès des autorités de poursuite pénale afin d'accomplir leurs tâches légales (art. 60 LP). De ce fait, la loi sur la protection des données, qui prévoit que des données peuvent être communiquées si cela est impérativement requis pour l'accomplissement d'une tâche légale, peut servir de base légale aux demandes émises dans ce contexte par les offices des poursuites.

1.10 International

1.10.1 Coopération internationale

L'internationalisation des traitements de données personnelles et les défis qu'elle entraîne pour le respect du droit à la protection des données rendent urgents l'adoption d'un cadre juridique universel contraignant et le renforcement de la coopération entre les autorités de protection des données. L'Union européenne, le Conseil de l'Europe et l'OCDE ont entamé leurs travaux de révision de leurs instruments juridiques afin de renforcer l'effectivité la protection des données. Nous avons participé activement aux travaux du Conseil de l'Europe, de l'OCDE, des Conférences européenne et internationale des commissaires à la protection des données, des instances de contrôle commune Schengen et Eurodac et de l'Association francophone des autorités de protection des données.

Conseil de l'Europe

L'année 2011 a marqué le 30e anniversaire de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Cela a été l'occasion pour le Conseil de l'Europe de dresser un bilan et de regarder vers l'avenir. Si l'objectif de la Convention, à savoir la garantie à toute personne physique, quelles que soient sa nationalité ou sa résidence, du respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant, demeure pertinent, il s'avère nécessaire d'adapter l'instrument à l'environnement informationnel et technologique actuel afin de renforcer l'effectivité de la protection des données. Ainsi, le comité consultatif de la Convention 108 (T-PD), sous la présidence du préposé fédéral suppléant, a poursuivi son travail de modernisation de la Convention (voir 18e rapport d'activités 2010/2011, ch. 1.10.1). Suite à une consultation publique, le comité a examiné un premier document de travail avec des propositions de modification de la Convention (www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_FR.asp?).

Le travail en cours repose sur la nécessité de garder la nature générale et simple de la Convention, d'en conserver l'approche technologiquement neutre et d'assurer la cohérence avec le cadre juridique européen. Il s'agit également de maintenir le caractère international, ouvert et contraignant de la Convention, laquelle répond actuellement le mieux au besoin d'un instrument universel. Les travaux s'orientent vers un renforcement du droit à la protection des données afin de (re)donner aux individus le contrôle

sur leurs données. La Convention devrait continuer de s'appliquer à tous les traitements des secteurs public et privé. Elle ne devrait plus se limiter aux traitements automatisés, mais s'étendre à l'ensemble des traitements quels que soient les moyens et procédés utilisés. Toutefois, les traitements effectués à des fins exclusivement personnelles ou domestiques se verront exclus du champ d'application. Les définitions seront revues et complétées.

Au niveau des principes de base de la protection des données, les contours du principe de proportionnalité pourraient être précisées, notamment sous l'angle de la minimisation des données et du choix des moyens de traitement. Une disposition énonçant les motifs pouvant légitimer un traitement des données sera introduite et il n'est pas exclu que le régime des données sensibles soit revu, notamment avec une extension du catalogue des données et une meilleure prise en compte du contexte dans lequel se déroule le traitement. Le comité examine également l'introduction des principes de responsabilité et de protection des données intégrée (privacy by design). Il envisage de renforcer les droits des personnes concernées (en particulier la transparence des traitements et le droit d'opposition). L'introduction d'une obligation de dénoncer les violations de sécurité au moins aux autorités de contrôle est également étudiée. Le rôle, les tâches et les compétences des autorités de contrôle devraient être précisées, notamment en vue de renforcer la coopération internationale non seulement sous l'angle de l'échange d'informations et de l'assistance, mais également pour permettre des interventions conjointes. Les critères de l'indépendance de ces autorités seront précisés. Les compétences du comité consultatif seront également revues, notamment pour permettre un contrôle préalable à l'adhésion et introduire un meilleur suivi de l'application de la convention par les Parties.

Enfin, tout en maintenant le principe de la libre circulation des informations entre Parties et l'exigence du niveau de protection adéquat, le régime des flux transfrontières sera adapté à la réalité du monde actuel (Internet, informatique en nuage, etc). Le comité pourrait finaliser un projet d'ici fin 2012 en vue de son adoption par le Comité des Ministres du Conseil de l'Europe. Dans ses fonctions de président du comité, le préposé fédéral suppléant a aussi eu l'occasion d'intervenir dans différents forums internationaux et de présenter l'avancement des travaux de modernisation de la Convention et d'en souligner les avantages dans l'optique de l'adoption d'un cadre juridique universel contraignant.

Le comité consultatif poursuit ses travaux de révision de la recommandation n° R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi et conduit une évaluation de l'application de la recommandation n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police. Sur la base des résultats de cette évaluation, il décidera de l'opportunité de revoir cette

recommandation. Il a également adopté un avis positif sur la demande de l'Uruguay d'adhérer à la Convention 108. Son adhésion devrait intervenir en 2012 et l'Uruguay deviendra ainsi le premier État non européen partie à la Convention.

Conférence européenne des commissaires à la protection des données

Le 5 avril 2011 s'est déroulée, à Bruxelles, la conférence annuelle de printemps des commissaires européens à la protection des données à l'invitation du Contrôleur européen à la protection des données et du président du groupe de travail de l'article 29. Cette conférence réunissait les autorités de protection des données des États membres de l'Union européenne et des pays tiers parties à la Convention 108. La conférence a porté principalement sur la révision du cadre juridique européen de la protection des données. La conférence a adopté une résolution mettant l'accent sur la nécessité d'adopter un cadre juridique global en matière de protection des données qui couvre les secteurs privé et public, y compris les secteurs de la police et de la justice (voir sur notre site www.leprepose.ch, sous Thèmes – Protection des données – Coopération internationale). La résolution souligne également la nécessité d'une approche cohérente dans les efforts de modernisation des différents cadres juridiques existants au sein de l'Union européenne, du Conseil de l'Europe et de l'OCDE. Les commissaires sont d'avis que ces développements devraient permettre d'améliorer le cadre actuel et d'assurer ainsi une protection plus efficace des droits des personnes concernant le traitement de leurs données personnelles. Les commissaires ont également décidé de mieux coordonner les activités dans le domaine de la sécurité et de la justice menées par le groupe de l'article 29 et le groupe de travail de la conférence européenne sur la police et justice.

Groupe de coordination du contrôle d'Eurodac

Le groupe de coordination du contrôle d´Eurodac (voir notre 18e rapport d'activités 2010/2011, ch. 1.10.1) s'est réuni le 21 octobre 2011 pour une séance à laquelle nous avons participé. Le premier thème abordé fut celui du système automatisé de comparaison des empreintes digitales Eurodac. On y a entre autres discuté du rapport sur la destruction prématurée des données dans ce système, rapport qui a entretemps été adopté par le groupe de coordination et publié sur le site web du Contrôleur européen de la protection des données (www.edps.europa.eu). Le prochain thème central devrait être la question des empreintes digitales illisibles.

Un autre thème abordé dans cette séance a été le nouveau système européen d'information sur les visas (VIS). Dans ce contexte aussi, la surveillance du système VIS incombe d'une part aux autorités de surveillance nationales, d'autre part au Contrôleur européen de la protection des données. Ces autorités coopèrent activement pour

assurer une surveillance coordonnée du système VIS et des systèmes nationaux. Le système VIS a pu être mis en service pour la première région le 11 octobre 2011. Celle-ci comprend six pays d'Afrique du Nord, à savoir l'Algérie, l'Égypte, la Libye, la Mauritanie, le Maroc et la Tunisie. Il est prévu par la suite d'étendre l'application du système VIS au Proche-Orient et, dans une phase ultérieure, à la région du Golfe. Le système VIS contient les empreintes digitales et photographies faciales des demandeurs de visa, donc des données biométriques. Il a pour objectif de simplifier et d'accélérer la procédure d'octroi des visas, mais aussi d'aider à prévenir la fraude et d'éviter que plusieurs demandes de visa ne puissent être déposées simultanément dans différents États membres (visa shopping). Comme indiqué lors de la réunion, le système a été mis en service sans problèmes majeurs et semble fonctionner de manière stable. La Suisse a également mis en service le système VIS et adapté le droit suisse en conséquence.

Groupe de travail police et justice

Le groupe de travail police et justice de la Conférence européenne des commissaires à la protection des données a pour mission de suivre les développements législatifs touchant au secteur de la police, notamment ceux relevant de l'acquis Schengen, et de coordonner les activités de surveillance entre les autorités nationales de protection des données. Dans ce contexte, il émet des avis et des prises de position. Nous avons participé aux différentes réunions de février, mars, juin et septembre 2011. Le groupe de travail a en particulier établi une méthodologie commune d'évaluation des risques préalable aux inspections de données afin de renforcer l'efficacité de la surveillance; cette méthodologie a permis de mettre en lumières cinq domaines de risques. Ces derniers doivent toutefois être reformulés de manière encore plus précise afin de permettre une meilleure comparaison internationale. Le groupe de travail développera une politique de surveillance définissant la manière d'agir sur la base des risques identifiés. En vue de la conférence de printemps 2012, le groupe a préparé un document de travail exposant les différentes options envisageables pour son futur.

Autorité de contrôle commune Schengen

L'autorité de contrôle commune Schengen (ACC) s'est réunie à quatre reprises en 2011. L'ACC a en particulier poursuivi ses activités de contrôle et planifié de nouvelles inspections. Le rapport concernant l'inspection sur les alertes relatives aux personnes recherchées pour l'arrestation aux fins d'extradition sera prochainement disponible. Il en est de même pour le rapport concernant l'inspection de suivi des recommandations émises lors du contrôle relatif aux données de personnes ou de véhicules intégrées dans le SIS aux fins de surveillance discrète ou de contrôle spécifique. En 2012, L'ACC mènera une inspection sur les droits d'accès au SIS I afin que la protection des données soit effective. À cette fin, le Secrétariat a élaboré un questionnaire qui a été restructuré

suite aux discussions qui ont eu lieu lors des séances. Dans le cadre de cette inspection, la sensibilisation et l'information des personnes seront également examinées. L'ACC conduira également une inspection de nature technique sur le contenu du SIS I et 4all qui sera menée par un groupe d'experts provenant de six pays. Le site internet de l'ACC a par ailleurs été mis à jour et est accessible à l'adresse suivante: http://schengen.consilium.europa.eu.

Groupe de travail européen sur le traitement de cas relevant de la protection des données

Lors de ses précédentes réunions, le groupe de travail européen sur le traitement de cas relevant de la protection des données («Case Handling Workshop»), mis en place par la Conférence européenne des Commissaires à la protection des données, s'est concentré sur quatre sujets. En octobre 2011, le groupe de travail, constitué de représentants de 29 autorités nationales de protection des données, a ainsi premièrement abordé les questions ayant trait aux cas transfrontières et à la manière dont les différentes autorités de protection des données géraient de tels cas. Dans un deuxième temps, la problématique des réseaux sociaux et d'internet a été traitée. La discussion a principalement porté sur l'informatique en nuage (cloud computing) et nos collègues nordiques en ont profité pour nous faire part des résultats du premier contrôle qu'ils ont effectué dans ce domaine. Il en ressort qu'il faut impérativement sensibiliser les entreprises et autorités aux dangers de ce système et les responsabiliser. La troisième thématique abordée par le groupe de travail est celle des méthodes de contrôle utilisées par les autorités de protection des données en fonction de leurs compétences légales respectives. Lors de la discussion, nous avons constaté que de nombreuses autorités de protection des données disposent dans leur législation nationale de mesures de sanctions sous forme d'amendes à l'encontre de l'organe contrôlé, ce que le droit suisse ne connaît pas actuellement. Enfin, la surveillance sur le lieu du travail a été thématisée et illustrée à l'aide des divers cas concrets tirés de la pratique des différentes autorités de protection des données. Ces exemples ont mis en lumière que le recours aux nouvelles technologies, notamment à la vidéosurveillance et à la biométrie, devenait de plus en plus fréquent et nécessitait un travail actif d'information et de sensibilisation.

Conférence internationale des commissaires à la protection des données et à la vie privée

La 33e conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue à Mexico City du 1er au 3 novembre 2011 à l'invitation de l'Institut fédéral de l'accès à l'information et de la protection des données (IFAI)

(www.privacyconference2011.org). Sous le thème de «Vie privée, l'ère universelle», la conférence a réuni quelque 700 participants provenant du monde entier et représentant 80 autorités de protection des données, des organisations non gouvernementales, l'industrie et la science, ainsi que les administrations publiques. Comme à l'accoutumée, la conférence se déroule en deux parties: l'une réservée aux seules autorités de protection des données accréditées, l'autre ouverte à l'ensemble des acteurs concernés; ces derniers y ont l'occasion d'échanger et de débattre sur les enjeux du moment en matière de protection des données et de vie privée, à savoir en particulier les défis découlant de l'internationalisation croissante des traitements de données personnelles, la problématique de l'amoncellement des données («big data»), l'informatique en nuage (cloud computing), la responsabilité sociale («accountability»), le droit à l'oubli, les développements législatifs, la certification, les failles de sécurité et la protection des données intégrée (privacy by design). Nous avons eu l'occasion d'intervenir lors de deux sessions plénières et de mettre l'accent sur l'apport de la Convention 108 dans le contexte international et le développement des différentes législations de protection des données à travers le monde.

S'il est réjouissant que le nombre d'Etats dotés de législations de protection des données ne cesse d'augmenter, nous avons souligné que pour garantir l'interopérabilité, il est important de fédérer et d'harmoniser les législations. Cela suppose l'adoption d'un cadre international contraignant reposant sur un standard commun. En l'absence de normes universelles contraignantes, la convention 108 est appelée ainsi à continuer de jouer un rôle fondamental et peut servir de base à un accord de portée universelle. Tout en rappelant qu'un cadre juridique contraignant est indispensable, nous avons également plaidé pour un renforcement de la coopération internationale, en particulier entre autorités de protection des données, ainsi que pour le développement du dialogue avec l'ensemble des acteurs de la société civile.

La conférence fermée des commissaires à la protection des données a mis l'accent sur la nécessité de renforcer la coopération entre les autorités de protection des données afin d'être plus efficace, notamment dans le cadre d'opération de contrôles. Elle a en particulier adopté une résolution sur la coordination de l'application des dispositions en matière de protection de la vie privée à l'échelle internationale. Elle souhaite également renforcer son rôle et a adopté à cet effet de nouvelles règles de procédures, créant notamment un comité exécutif, lequel sera présidé par le président de l'autorité de protection des données des Pays-Bas. La conférence fermée a en outre adopté une résolution sur la protection des données et les catastrophes naturelles et une

résolution sur l'utilisation à un identifiant unique dans le déploiement du protocole Internet version 6 (IpV6). Cette résolution plaide en particulier pour le maintien par défaut d'adresses IP dynamiques.

Les résolutions se trouvent sur notre site www.leprepose.ch, sous Thèmes – Protection des données – Coopération internationale.

Groupe de travail sur la sécurité de l´information et la vie privée (OCDE)

Le groupe de travail s´est penché sur la révision des directives relatives à la sécurité et à la protection des données, sur la question du caractère économique des données personnelles en rapport avec la protection et la sécurité des données, sur les possibilités d´utilisation de données médicales dans la recherche et sur le renforcement de la protection des données et de la sécurité sur Internet. Il a également abordé quelques autres sujets tels que les stratégies nationales en matière de sécurité de l´information et de lutte contre la cybercriminalité, et finalement la révision des lignes directrices sur la sécurité des réseaux d´information.

L´évolution fulgurante dans le domaine de la vie privée, en particulier le stockage et le dépouillement transfrontière d´un volume de données personnelles sans précédent, aura marqué les discussions relatives à la révision de la directive sur la sécurité et la protection des données. Étant donné que les réglementations nationales touchent à leurs limites d´intervention, l´utilisation de technologies respectueuses de la protection des données est considérée comme essentielle pour améliorer la protection de la sphère privée sur Internet. Par conséquent, un groupe d´experts a été mis en place pour examiner de quelle manière les principes fondamentaux de la directive pourraient être modifiés. Ces experts soumettront leurs propositions de modification au groupe de travail.

Le rôle des données personnelles sur Internet est également pertinent si l´on considère le caractère économique de l´information du point de vue de la protection des données et de la sécurité. Pour répondre à la question de savoir quel prix est à attribuer aux données personnelles, il est prévu d´effectuer des calculs correspondants dans quatre domaines sélectionnés (réseaux sociaux, sociétés de renseignements commerciaux, moteurs de recherche et programmes de fidélisation des clients). Cela devrait également répondre à la question de savoir dans quelle mesure les données personnelles peuvent entraver l´innovation technologique. Il ne s´agit cependant pas de conclure à un niveau de protection des données plus ou moins élevé uniquement sur la base de critères économiques. Au contraire, il importera de définir les dangers pour la vie privée et, le cas échéant, de proposer des mesures qui puissent être mises en œuvre par des

entreprises ou des autorités. Il n´est pas acceptable de prendre comme unique critère l´appréciation que les citoyens font eux-mêmes de leurs données personnelles, étant donné qu´ils les sous-estiment souvent en raison du manque d´information et de sensibilisation. Il y a donc lieu de prendre en compte lors de cette évaluation le fait que les moteurs de recherche ou les réseaux sociaux par exemple collectent le maximum possible de données. Enfin, des champs de données isolés tels que l´adresse ou le numéro de téléphone n´ont pas la même valeur qu´une combinaison de ces champs ou les profils qui en résultent. Une étude externe mandatée devra répondre à la question du prix des données personnelles. Elle devra tenir compte des différents modes de calcul.

En ce qui concerne l´utilisation de données personnelles dans la recherche médicale, le Comité santé a présenté les premières étapes. Il s´agit en premier lieu de pouvoir utiliser de manière plus efficace les données médicales à des fins de recherche, tout en tenant compte des implications que ceci a sur la vie privée des patients affectés. S´ajoute à cela que, dans la plupart des pays européens, il existe déjà un cadre réglementaire détaillé pour le traitement des données personnelles dans le domaine médical. Ceci n´empêche pas d´étudier toutes les possibilités permettant de faciliter l´utilisation des données. Un groupe d´experts sera mis sur pied à cet effet et accordera une attention particulière aux implications sur la vie privée.

Compte tenu des récentes attaques pirates et de l´accroissement de la criminalité sur Internet, la question de la sécurité de l´information reste un thème d´actualité. Plusieurs pays de l´OCDE ont déjà élaboré des stratégies nationales pour lutter contre la cybercriminalité et renforcer la sécurité de l´information. Le groupe de travail réunira maintenant ces diverses stratégies nationales dans une étude comparative. Cette étude servira ensuite de point de départ pour la réflexion sur la manière la plus efficace d´assurer la sécurité des réseaux d´information au niveau international.

Enfin, dans la foulée, le groupe de travail examinera s´il est nécessaire de réviser les directives datant de 2002 sur la sécurité des réseaux d´information.

Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP) a tenu sa cinquième conférence à Mexico City, le 31 octobre 2011. Elle a été suivie de l'Assemblée générale de l'Association. En outre, l'Association a organisé deux jours de séminaire de formation à l'intention de ses membres, à Dakar les 20 et 21 septembre 2011. Ce séminaire a été précédé de la première rencontre régionale africaine sur la protection des données organisée par l'AFAPDP.

Ces diverses manifestations ont été l'occasion d'un vaste échange entre les «anciennes» autorités de protection des données et les autorités nouvellement installées

ou en cours d'installation. Ces échanges ont pour l'essentiel porté sur les technologies de l'information et des communications, la biométrie, la responsabilité des entreprises, les flux transfrontières de données, la coopération entre autorités, les politiques de formation et de sensibilisation, ainsi que les développements en matière de protection des données en Afrique. Lors de la cinquième conférence, nous avons eu l'occasion de présenter les avantages d'une adhésion à la convention 108, notamment dans l'optique des échanges d'informations entre l'Union européenne et les pays tiers, ainsi que les conditions requises pour une telle adhésion.

Lors de son assemblée générale, l'AFAPDP a adopté quatre résolutions. La première concerne le développement d'un référentiel de principes communs aux autorités francophones pour encadrer les transferts de données personnelles entre entreprises. Ce référentiel doit permettre aux autorités de disposer d'un cadre permettant d'apprécier dans la pratique le caractère adéquat de la protection apportée aux transferts de données. La deuxième résolution porte sur la sensibilisation efficace de la société à la protection des données. Une troisième résolution a trait à l'indépendance des autorités de protection des données. Elle rappelle en particulier que «seule une autorité strictement indépendante dispose de l'objectivité et de l'impartialité nécessaires à la défense des droits fondamentaux et libertés individuelles à l'égard de données personnelles.» Elle énonce également certains critères propres à garantir cette indépendance (base légale, absence d'instruction, modalités de nomination, autonomie budgétaire, mise à disposition de moyens suffisants, liberté dans le recrutement du personnel). Enfin, la quatrième résolution adoptée concerne l'utilisation de la langue française à la conférence internationale des commissaires à la protection des données et à la vie privée. Adressée à la 33e conférence, l'AFAPDP y fait part de sa préoccupation par rapport à l'exclusion croissante de l'usage du français, langue commune à plus de 70 États, de la conférence internationale. Avec l'appui du Réseau ibéro américain de protection des données, également concerné par l'exclusion de la langue espagnole, l'AFAPDP a obtenu que, l'interprétation du français et de l'espagnol soit assurée lors des prochaines conférences, au besoin avec l'aide des différentes communautés linguistiques.

Les résolutions se trouvent sur notre site www.leprepose.ch, sous Thèmes – Protection des données – Coopération internationale.

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

Le groupe de travail international sur la protection des données dans le domaine des télécommunications, dit «Groupe de Berlin», s'est réuni en avril et en septembre 2011. Depuis plusieurs années, la protection des données dans les réseaux sociaux est pour lui un thème permanent. Il s'est également penché sur les derniers développements de la technique et sur les risques qu'ils impliquent en termes de protection de données, en particulier sur l'utilisation des technologies de reconnaissance faciale sur Internet.

En outre, des documents de travail ont été adoptés à propos de la protection des données liée à l'utilisation des compteurs électriques intelligents (smart metering), au micropaiement électronique sur Internet ainsi qu'à l'enregistrement de données dans les véhicules. Pour sa part, l'informatique en nuage (cloud computing) a pour l'heure fait l'objet d'un document de travail assorti de recommandations qui devrait être adopté au cours de la prochaine rencontre du groupe, en avril 2012.

Les documents publiés par le Groupe de Berlin peuvent être consultés sur Internet: www.iwgdpt.org ou www.datenschutz-berlin.de sous Europa/International – International Working Group on Data Protection in Telecommunications (IWGDPT), en anglais et en allemand.

2. Principe de la transparence

2.1 Demandes d'accès

2.1.1 Départements et offices fédéraux

Le nombre des demandes d'accès déposées a presque doublé par rapport à l'année précédente. Par contre, le pourcentage des accès accordés et des accès refusés est resté stable. Le nombre des demandes de médiation a lui aussi doublé. On enregistre en outre une augmentation conséquente des émoluments demandés par les autorités.

Selon les chiffres qui nous ont été communiqués, 466 demandes d´accès ont été déposées auprès des autorités fédérales en 2011. Dans 203 cas, les autorités ont accordé un accès complet et dans 128 cas un accès partiel. Dans 126 cas, l'accès aux documents a été totalement refusé. Un fait frappe au premier regard: les chiffres ont pratiquement doublé par rapport aux années précédentes (voir la statistique figurant au chiffre 3.5). En premier lieu, cette augmentation découle probablement du fait que l'écho de la loi sur la transparence auprès du public est de plus en plus grand, surtout auprès des professionnels des médias, et que les demandes d'accès sont de plus en plus fréquentes. D'autre part, il est permis de supposer que cinq ans après l'entrée en vigueur de la loi sur la transparence, les autorités sont davantage sensibilisées à la question et qu'elles ont commencé à répertorier systématiquement les demandes d'accès et à établir des statistiques. Par contre, on ne relève aucun changement par rapport à l'année précédente pour ce qui est du pourcentage des refus complets (27%), des refus partiels (27%) et des accès entièrement accordés (44%).

C'est l'Office fédéral de la santé publique (OFSP) qui nous a transmis le plus grand nombre de demandes d'accès pour l'année 2011 (33 demandes), suivi de l'Inspection fédérale de la sécurité nucléaire (IFSN) et de l'Office fédéral de l'environnement (OFEV) avec chacun 22 demandes, un lien direct avec Fukushima étant probable du moins pour l'IFSN. Parmi les départements, le DETEC (110 demandes d'accès), le DFI (87) et le DFAE (80) sont en tête. Sur 71 autorités, 13 nous ont informés qu'elles n'avaient reçu aucune demande d'accès pour l'année 2011.

La tendance – déjà constatée au cours de l'année précédente – que les autorités font davantage usage de la possibilité prévue par la loi sur la transparence de prélever des émoluments s'est poursuivie durant l'année 2011. Selon les chiffres qui nous ont été remis, onze offices ont facturé des émoluments pour un montant total de 13'140 francs. En comparaison avec les années précédentes, cela constitue une augmentation conséquente de presque 10'000 francs (3460 francs en 2010 et 3850 francs en 2009).

En ce qui concerne la charge de travail occasionnée par les demandes d'accès remises à l'administration fédérale, nous soulignons cette année encore que d'abord, les autorités ne sont pas tenues de noter les heures consacrées et qu'ensuite, il n'existe aucune directive sur une saisie uniforme du temps de travail dans ce domaine qui soit applicable à l'ensemble de l'administration fédérale. Les données nous sont transmises sur une base volontaire et ne sont donc pertinentes que jusqu'à un certain point. Selon ces chiffres donc, la charge de travail a continué d'augmenter (2009: 748 heures; 2010: 815 heures, 2011: 1519 heures). Les heures consacrées à la participation à des procédures de médiation est passée de 158 heures en 2010 à 453 heures en 2011.

2.1.2 Services parlementaires

Selon les renseignements fournis par les services parlementaires, une seule demande leur a été adressée en 2011, suite à laquelle l'accès a été entièrement accordé.

2.1.3 Ministère public de la Confédération

Le Ministère public de la Confédération nous a informés que dans deux cas, il avait entièrement accordé l'accès demandé et que dans un cas, il l'avait entièrement refusé.

2.2 Demandes en médiation

En 2011, nous avons reçu un total de 65 demandes en médiation (voir la statistique au chiffre 3.8), ce qui représente deux fois plus que l'année précédente (32). La plupart ont été déposées par des professionnels des médias (24 demandes), suivis par des entreprises (16).

En tout, 30 demandes en médiation ont été menées à terme. Dans huit cas, une solution consensuelle a été trouvée entre les parties impliquées. Dans neuf cas, nous avons émis des recommandations car une solution à l'amiable n'a pu être trouvée ou était d'emblée inenvisageable. Parfois, nous avons pu clore plusieurs demandes avec une seule recommandation ou une seule médiation. Dans cinq cas, les offices ont accordé de leur propre chef l'accès pendant la procédure de médiation en cours. Deux demandes ont été retirées et dans quatre cas, les conditions d'application de la loi sur la transparence n'étaient pas données. Enfin, dans deux cas, la demande en médiation a été déposée en dehors des délais.

Ces chiffres permettent d'émettre les conclusions et les remarques suivantes:Dans 254 cas, l'administration fédérale a refusé l'accès complètement (126) ou ne l'a accordé que partiellement (128). Suite à ces refus complets ou partiels, 65 demandes en médiation ont été déposées chez nous. Cela signifie donc que dans à peine 26% des accès entièrement ou partiellement refusés, nous avons par la suite reçu une demande en médiation. Dans 15 cas sur 17, les procédures en médiation ont été menées à terme avec une médiation ou une recommandation et nous avons réussi à obtenir une solution plus favorable pour le requérant (à savoir une médiation ou un accès plus étendu que celui qui avait à l'origine été accordé par l'office fédéral).

Grâce à la révision partielle de l'ordonnance sur la transparence (OTrans) entrée en vigueur en juillet 2011, nous pouvons désormais prolonger de manière adéquate le délai permettant de mener les procédures de médiation qui nécessitent un important surcroît de travail. Mais indépendamment de cela, les requérants doivent attendre plus longtemps avant que la procédure soit engagée d'une part parce que le nombre des demandes déposées a considérablement augmenté durant l'année sous revue, mais aussi parce que nous ne disposons toujours pas de ressources suffisantes pour les traiter.

2.3 Procédures de médiation closes

2.3.1 Recommandations

Les recommandations émises au cours de l'année écoulée concernant la loi sur la transparence sont résumées ci-dessous. Ces recommandations peuvent être consultées dans leur version intégrale sur notre site Internet www.leprepose.ch, sous la rubrique Documentation – Principe de la transparence – Recommandations.

Recommandation OFEV / Analyse de carburants (16 mai 2011)

La demanderesse a déposé auprès de l'Office fédéral de l'environnement (OFEV) une demande d'accès aux résultats d'analyse des carburants (essence et diesel) dans les stations service. L'OFEV a consenti un accès anonymisé aux données pertinentes au regard de l'ordonnance sur la protection de l'air (OPair), mais a refusé l'accès aux autres données. Il faisait valoir d'une part que la confidentialité avait été garantie aux entreprises concernées et d'autre part que les rapports d'analyses étaient soumises au secret d'affaires de ces entreprises. Il affirmait en outre qu'il était impossible de rendre ces données anonymes. Le préposé a établi dans ses conclusions que la garantie du secret n'avait pas été donnée expressément et qu'en outre, les rapports d'analyse ne contenaient pas de secret d'affaires. Selon l'estimation du préposé, il était tout à fait possible de rendre anonymes les données personnelles figurant dans les documents demandés. Il a de ce fait recommandé que les rapports d'analyse soient rendus accessibles sous une forme anonymisée.

Recommandation CFF / Concept d'exploitation (1er juillet 2011)

Dans le cadre de la planification de la quatrième extension partielle du RER Zurich, la demanderesse a requis des Chemins de fer fédéraux (CFF) le «concept d'exploitation de la gare d'Herrliberg-Feldmeilen». Les CFF ne lui ayant pas remis le document souhaité, la demanderesse a déposé une demande en médiation. Le préposé a constaté dans sa recommandation que dans le domaine de la construction d'installations ferroviaires, les CFF n'avaient pas la compétence de fixer des règles de droit ni de rendre de décisions et que de ce fait, la loi sur la transparence n'était pas applicable.

Recommandation OFC / Rapport Analyse et exploitation d'un projet pilote (4 juillet 2011)

Le demandeur a requis de l'Office fédéral de la culture (OFC) l'accès au rapport d'analyse et d'exploitation d'un projet pilote. L'OFC a tout d'abord refusé l'accès à ces documents, en arguant qu'ils allaient encore servir de base à d'autres négociations. L'office a transmis plus tard l'information selon laquelle ces négociations avaient été menées; il persistait néanmoins dans son refus d'accorder l'accès à ces documents au motif que cela entraverait les mesures concrètes prises par certaines autorités, en l'occurrence fedpol. À la suite de quoi le préposé a demandé à plusieurs reprises à fedpol de lui fournir des informations permettant de clarifier l'applicabilité de la loi sur la transparence, en vain. En définitive, le préposé a recommandé l'accès au rapport requis sous une forme partiellement anonymisée.

Recommandation SECO / Contributions aux frais d'exécution de la CPN (6 juillet 2011)

En ce qui concerne les activités de surveillance du Secrétariat à l'économie (SECO) dans le cadre de la convention collective de travail dans la branche suisse des techniques des bâtiments, la demanderesse a requis l'accès aux comptes annuels, aux budgets et aux rapports de révision de la Commission paritaire nationale (CPN) de la branche de la technique du bâtiment. Le SECO a refusé cet accès en invoquant le fait que les documents demandés renfermaient des secrets d'affaires et que la sphère privée de tiers s'en trouverait atteinte. D'après les estimations du préposé, les documents demandés ne contiennent pas de secrets d'affaires. S'agissant des données personnelles, il a recommandé d'en rendre une partie anonymes et d'en permettre l'accès à l'autre partie en raison de la présence d'un intérêt public prépondérant.

Recommandation OFAG / Formulaires de contrôle des quantités de lait supplémentaires (5 août 2011)

Le demandeur a requis l'accès aux formulaires de contrôle des quantités de lait supplémentaires autorisés par l'Office fédéral de l'agriculture (OFAG). L'OFAG a remis à la demanderesse 67 formulaires dont certaines données, comme les noms des transformateurs de lait, les produits et les numéros d'identification des groupes de produits, avaient été caviardées. L'office refusait en outre l'accès aux formulaires de cinq grands transformateurs de lait et invoquait la protection des secrets d'affaires et des données personnelles. Sur ce, le demandeur a donc déposé une demande en médiation. Au cours de la procédure de médiation, le préposé est parvenu à la conclusion que les données figurant sur ces cinq formulaires permettaient bien en définitive de déduire les stratégies d'exportation des transformateurs de lait. Étant donné que les

transformateurs de lait sont entre eux en situation de concurrence, on ne pouvait pas exclure que la divulgation de ces informations n'ait effectivement des répercussions négatives sur les stratégies de marché de l'un en particulier et ne crée des distorsions de concurrence. Selon les estimations du préposé, ces cinq transformateurs de lait avaient de ce fait à la fois un intérêt légitime et un intérêt digne de protection à ne pas permettre l'accès à ces informations. Dans ces circonstances, le préposé a qualifié les données figurant sur les formulaires de contrôle de secrets d'affaires et a soutenu l'OFAG dans sa décision de ne pas octroyer l'accès aux données en question.

Recommandation AFC / Cockpits et Amtsreportings (19 septembre 2011)

Suite au jugement rendu par le Tribunal administratif le 15 septembre 2009 concernant les documents désignés par les appellations de «Cockpits» et de «Amtsreportings», l'Administration fédérale des contributions (AFC) a fait parvenir au demandeur les documents demandés en partie caviardés. L'AFC ne justifiait ce passage à l'encre noire ni dans les documents, ni dans la lettre d'accompagnement; les raisons du caviardage étant incompréhensibles pour le demandeur, celui-ci a donc déposé une demande en médiation. Au cours de la procédure de médiation, l'AFC a expliqué au préposé l'utilisation de l'encre noire et déclaré accessibles certains passages supplémentaires. Par contre, elle a refusé l'accès à d'autres passages au motif que cela entraverait la libre formation de l'opinion et de la volonté, la mise en œuvre de mesures décidées par les autorités conformément aux objectifs fixés, ainsi que la sphère privée de tiers et d'employés de l'administration. Néanmoins, des divergences existaient encore entre l'AFC et le préposé à propos des passages caviardés. D'une part, le préposé a recommandé l'accès à certains passages, contrairement à l'avis de l'AFC, d'autre part il a soutenu l'avis de l'AFC selon lequel dans des cas déterminés, l'accès ne peut pas être accordé ou peut être ajourné, par exemple lorsqu'il s'agit de données de tierces personnes et d'employés de la Confédération.

Recommandation OFEN / Procès-verbaux de la CSN (16 décembre 2011)

Le demandeur a requis auprès de l'Office fédéral de l'énergie (OFEN) l'accès à tous les procès-verbaux de séance de la Commission fédérale de sécurité nucléaire (CSN) pour l'année 2009. L'OFEN et le demandeur ont convenu de la remise d'un seul procès-verbal, ce qui fut fait, mais le procès-verbal était caviardé sur de larges passages. L'OFEN a motivé l'utilisation du caviardage par le fait qu'une divulgation des données en question mettrait en danger des décisions politiques et administratives encore en suspens. La procédure de médiation a réuni le préposé, l'OFEN et la CSN. Afin de pouvoir librement discuter du contenu des passages caviardés, cette réunion a eu lieu sans le demandeur. Le préposé a donné son avis sur chacun des passages en question, sous

l'angle de l'acceptation ou du refus de l'accès. Sur la base de ces discussions et des décisions politiques et administratives prises entre temps, l'OFEN et la CSN se sont déclarés d'accord de permettre l'accès à la plupart des paragraphes incriminés et de ne recouvrir d'encre noire que deux petits passages. En ce qui concerne ces passages, le préposé a convenu avec l'OFEN et la CSN que leur accès serait repoussé jusqu'à ce que la décision politique et administrative soit prise.

Recommandation BAG / Tarifs de primes LAMal (19 décembre 2011)

Le demandeur a requis de l'Office fédéral de la santé publique (OFSP) l'accès aux tarifs de prime soumis et approuvés des assurances-maladie, ainsi que les décisions de non-approbation. L'Office fédéral a remis au demandeur en tout quatre documents de deux assurances-maladie, dans leur version intégrale, mais a refusé un accès plus large au motif que les documents restants contenaient soit des informations qui étaient déjà contenues dans les documents déjà remis, soit des secrets d'affaires. En outre, il refusait l'accès aux documents concernant les deux autres assurances-maladies au motif qu'ils n'étaient pas inclus dans la demande d'accès du fait de leur date. Cet avis a été approuvé par le préposé dans la procédure de médiation. Pour ce qui est des autres documents, le préposé a qualifié de secrets d'affaires les calculs budgétaires et les informations sur la situation financière et s'est rangé à l'avis de l'OFSP selon lequel il fallait ici refuser l'accès. Enfin, pour le reste, il a recommandé un accès partiel.

Recommandation OFAS / Procès-verbaux de séance de la Commission fédérale de l'AVS/AI (22 décembre 2011)

Le demandeur a requis auprès de l'Office fédéral des assurances sociales (OFAS) l'accès à plusieurs procès-verbaux des séances de la Commission fédérale de l'AVS/AI de l'année 2009. L'OFAS a refusé l'accès à ces documents au motif qu'en tant que commission administrative, celle-ci n'entrait pas dans le champ d'application de la loi sur la transparence, à raison des personnes, que les séances étaient confidentielles et que les documents contenaient des données personnelles.

Au cours de la procédure de médiation, le préposé a attiré l'attention de l'OFAS sur le jugement passé en force du Tribunal administratif fédéral du 17 juin 2011 dans lequel il avait été décidé que les commissions d'administration appartenaient aussi depuis le 1er janvier 2009 à l'administration fédérale décentralisée et entraient donc dans le champ d'application de la loi sur la transparence. L'OFAS a maintenu sa position. Mais cet office n'étant pas en mesure de présenter de motifs d'exception, le préposé a recommandé l'accès aux procès-verbaux de séance.

2.3.2 Médiations

Nous avons trouvé une solution consensuelle dans les cas suivants:

Médiation OFEN / Documents concernant les éclusées du barrage de Châtelot

Le demandeur a demandé à l'Office fédéral de l'énergie (OFEN) l'accès à des documents législatifs et contractuels concernant l'exploitation par éclusée du barrage de Châtelot. L'OFEN a renvoyé le demandeur d'une part à un communiqué de presse, d'autre part à la compétence des autorités françaises. Dans sa prise de position à l'intention du préposé, l'office a refusé l'accès à quatre documents au motif que ceux-ci avaient été établis avant l'entrée en vigueur de la loi sur la transparence. En ce qui concerne les autres documents, l'OFEN se référait à des négociations en cours ou futures concernant, outre la Confédération, plusieurs autorités cantonales ainsi que la France. Au cours de la procédure de médiation, les parties ont déterminé l'ampleur des documents pertinents qui intéressaient le demandeur et se sont mis d'accord sur la suite à donner à la requête.

Médiation OFPP / Rapport Polycom

Le demandeur a requis de l'Office fédéral de la protection de la population (OFPP) l'accès au rapport «Polycom : Vision im Bereich IKT, Analyse und Konzept». L'OFPP a répondu au demandeur entre autres que le rapport n'était pas terminé. Suite à l'intervention du préposé et après la prise de contact de l'OFPP avec plusieurs organes fédéraux, l'OFPP a accordé au demandeur l'accès partiel au document en question.

Médiation OFAS / Versements de subventions

Le demandeur a requis de l'Office fédéral des assurances sociales (OFAS) la consultation de documents concernant des subventions que la Confédération avait versées en 2007 à des institutions possédant des homes et des ateliers pour handicapés. Étant donné le grand nombre de ce genre d'institutions et le montant des émoluments liés à la demande d'accès, le demandeur s'est limité à 35 institutions. Tout en reconnaissant en principe l'intérêt prépondérant que revêt l'accès à une liste des versements de subventions, l'OFAS a invoqué l'obligation de consulter les institutions concernées. Le demandeur, lui-même une institution disposant d'un home et d'un atelier, ne voulait toutefois pas dévoiler son identité. C'est pourquoi il s'est mis d'accord avec l'OFAS pour que sa demande d'accès ne concerne que les institutions qui consentiraient à

la publication de leur décision de subvention à cette condition. Au cas où une institution ne donnerait pas son accord, il retirerait sa demande d'accès; ainsi le demandeur a renoncé à l'émission d'une décision qui lui aurait été notifiée, à lui et à l'institution concernée.

Médiation CDF/ Rapport de contrôle

Le demandeur a requis du Contrôle fédéral des finances (CDF) l'accès à deux rapports de contrôle concernant le bureau de coopération au Tchad. Le CDF a reconnu le droit fondamental à la consultation de ces documents. Sur la base de la complexité du cas (entre autres l'audition de personnes à l'étranger) et de la charge de travail qui en découlerait, le CDF a informé le demandeur qu'il devait s'attendre à des émoluments de plusieurs milliers de francs. Dans le cadre de la procédure de médiation, le demandeur et le CDF ont convenu que ce dernier anonymiserait, selon sa propre appréciation, toutes les données personnelles ou caviarderait des paragraphes entiers contenant des données personnelles; ils se sont également mis d'accord sur un montant d'émoluments de 500 francs (pour le travail fourni jusque-là).

Médiation DDPS / Liste des appartements des attachés de défense

La demanderesse désirait obtenir une liste des appartements des attachés de défense, avec indication des coûts de location ou d'achat. Elle a contacté à cet effet certains services administratifs du DFF et du DDPS, mais l'accès au document en question ne lui a pas été accordé, notamment pour des raisons de sécurité. Une fois la question de la compétence réglée au cours de la procédure de médiation, le DDPS s'est déclaré prêt à fournir à la demanderesse la liste souhaitée avec les frais de location des appartements, les adresses ayant toutefois été passées à l'encre noire. La demanderesse a retiré sa requête concernant les frais d'achat des appartements à Stockholm et Washington.

Médiation ODM / Contrat avec une garderie d'enfants

L'Office fédéral des migrations (ODM) avait conclu avec une personne privée une déclaration d'intention et un contrat en vue de l'établissement d'une garderie dans laquelle des places seraient garanties aux enfants des employés de l'ODM. Une autre garderie d'enfants a demandé accès à ces documents, ce que l'ODM a toutefois refusé. Suite à la procédure de médiation, le préposé a estimé que l'accès à ces documents devait être garanti et a suggéré que la personne privée soit consultée. Celle-ci a consenti à la publication des documents en question.

Médiation IFSN/ Fissures dans le manteau du cœur du réacteur de la CNM

La demanderesse a requis l'accès aux résultats des analyses concernant l'état du manteau du cœur du réacteur de la Centrale nucléaire de Mühleberg (CNM) ainsi que les critères présidant à ces analyses et à l'entretien des fissures dans le manteau du cœur du réacteur de la CNM. L'Inspection fédérale de la sécurité nucléaire (IFSN) a refusé l'accès aux documents demandés au motif que leur divulgation porterait atteinte à la libre formation de son opinion et de sa volonté et que la décision sur le rapport sur l'exploitation à long terme de la centrale était encore attendue. La procédure de médiation a permis aux parties, avec le soutien du préposé, d'une part de limiter le volume des documents sur les fissures dans le manteau du cœur du réacteur, d'autre part de se mettre d'accord pour que l'IFSN permette l'accès à des passages de documents répondant aux questions centrales de la demanderesse.

Médiation ChF / Vote électronique

Le demandeur a requis auprès de la Chancellerie fédérale (CF) la possibilité de consulter tous les documents du Conseil fédéral et de la Chancellerie fédérale concernant l'approbation par le Conseil fédéral de l'utilisation du vote électronique pour les élections au Conseil national de 2011 et pour les préparations du vote électronique lors des élections de 2007; elle désirait aussi avoir accès à une liste de tous les documents relatifs au vote électronique dans le système électronique des affaires (GEVER) depuis 2007. La Chancellerie a refusé l'accès à ces documents au motif que la loi sur la transparence n'était pas applicable aux documents du Conseil fédéral; elle estimait en outre qu'octroyer un accès à ces documents porterait atteinte à la sécurité intérieure et à la relation avec les cantons. Elle demandait par ailleurs au demandeur que le large spectre sur lequel portait la demande soit précisé. Au cours de la procédure de médiation, la ChF a maintenu sa position pour l'essentiel, mais s'est montrée prête à recevoir la demanderesse pour deux entretiens afin de l'informer entre autres «du point de vue de la Confédération» sur les questions de sécurité entre le vote proprement dit et la publication des résultats.

2.4 Décisions judiciaires relatives à la loi sur la transparence

2.4.1 Tribunal administratif fédéral

Au cours de l'année écoulée, le Tribunal administratif fédéral (TAF) a rendu quatre arrêts suite à des procédures de médiation auprès du préposé.

Ainsi, le TAF a décidé que les conventions de résiliation des contrats de travail de l'ancien secrétaire général du Département fédéral de justice et police (DFJP) et de son suppléant devaient pouvoir être consultées par le public.

Le Tribunal a accordé un poids plus grand aux intérêts du demandeur (et donc aux intérêts du public) à consulter ces conventions qu'à ceux des deux personnes concernées à la protection de leur sphère privée (voir l'arrêt du 17 février 2011, réf. A-3609/2010). Le Tribunal fédéral avait renvoyé ce cas pour réexamen devant le TAF (voir notre 18e rapport d'activités 2010/2011, ch. 2.4.1).

Conformément au TAF, la liste des déclarations d'intérêts concernant les membres de la Commission fédérale pour les vaccinations (CFV) doit pouvoir être consultée par le public. C'est ce qu'il ressort de l'arrêt rendu par le Tribunal administratif fédéral le 17 juin 2011. Selon cet arrêt, l'intérêt de la demanderesse à pouvoir consulter la liste prévaut sur celui des membres concernés de la commission à la protection de leur sphère privée (voir l'arrêt du 17 juin 2011, réf. A-3192/2010).

En vue d'un éventuel accord de libre-échange entre la Suisse et l'Union européenne dans le secteur agro-alimentaire, le Département fédéral de l'économie (DFE) a mis sur pied en 2008 un groupe de travail ad hoc chargé d'élaborer des mesures d'accompagnement concrètes. Selon un jugement du TAF, ce groupe de travail doit être considéré comme faisant partie de l'administration fédérale et doit par conséquent est soumis à la loi sur la transparence. Il a donc été enjoint à l'Office fédéral de l'agriculture (OFAG) d'octroyer à la journaliste l'accès à un document du groupe de travail contenant 250 propositions pour des mesures d'accompagnement. Selon cet arrêt, les membres du groupe ne peuvent pas faire valoir d'une façon générale la protection de leur sphère privée (arrêt du 7 décembre 2011, réf. A-1135/2011).

Dans le quatrième cas, il s'agissait d'une interview que l´ancienne conseillère fédérale Micheline Calmy-Rey avait accordée à un quotidien. Celui-ci avait convenu avec le Département fédéral des affaires étrangères (DFAE) de communiquer l'interview au DFAE pour d'éventuelles rectifications. Un demandeur a requis l´accès à ce document, ce que le DFAE a refusé. Le préposé s'est rallié à cette position dans sa recommandation

du 9 décembre 2010, à la suite de quoi le demandeur a déposé recours contre cette décision. Le TAF a donné raison au DFAE et établi dans son jugement que seule la version définitive corrigée sans corrections visibles doit être considérée comme un document définitif et donc comme un document officiel (arrêt du 22 décembre 2011, réf. A-1156/2011).

2.5 Consultation des offices

2.5.1 Révision de la loi sur les cartels

Le préposé s'est prononcé sur la révision de la loi sur les cartels. Cette révision a entre autres pour but de soumettre les autorités en matière de concurrence à une réorganisation et de créer un nouveau Tribunal de la concurrence (dans le cadre d'une réforme institutionnelle). Il est également prévu à cet égard de retirer partiellement les autorités de la concurrence du champ d'application matériel de la loi sur la transparence (LTrans). Concrètement, cela signifie que dorénavant, les procédures visant à juger les restrictions à la concurrence, c'est-à-dire les recherches préalables et les enquêtes, ne seraient plus couvertes par la LTrans. Le motif invoqué ici est qu'il serait inconséquent de soumettre les dossiers de procédure des autorités de la concurrence à la LTrans si plus tard, devant le Tribunal de la concurrence, les mêmes documents ne tombent plus dans le domaine d'application de cette même loi. En outre, pour les entreprises concernées, les documents en question revêtiraient un besoin de protection considérable. Pour ces raisons, cette procédure devait être retirée du champ d'application matériel de la LTrans.

Le préposé ne partageait pas cet avis et a remis au SECO une prise de position dans ce sens. D'une part, la loi sur la transparence offre, dans des cas particuliers, des possibilités légales suffisantes pour refuser l'accès à des documents, à le limiter ou à le repousser dans le temps, notamment en ce qui concerne la protection des secrets professionnels, d'affaires et de fabrication ainsi que des données personnelles. d'autre part, le préposé est tout à fait conscient du besoin accru de protection de certains documents officiels (par ex. dont le contenu concerne des secrets professionnels, d'affaires et de fabrication) et en a toujours tenu compte par le passé. Enfin, il ne faut pas oublier que la Commission de la concurrence actuelle (COMCO) et son secrétariat sont entièrement soumises à la LTrans depuis son entrée en vigueur. Durant tout ce temps, la COMCO n'a reçu que très peu de demandes d'accès. Cela montre que par le passé, la loi sur la transparence n'a ni rendu plus difficile les tâches des autorités de la concurrence, ni causé un surcroît de travail administratif.

De l'avis du préposé, il n'y avait donc aucun motif de retirer les nouvelles autorités de la concurrence en partie du champ d'application matériel de la LTrans. Mais le SECO n'ayant montré sur ce point aucune volonté de compromis, le préposé a établi un rapport à l'adresse du Conseil fédéral dans lequel il a de nouveau motivé sa position en détail. Le Conseil fédéral s'est en définitive rangé à l'avis du préposé et a décidé que les nouvelles autorités de la concurrence doivent, comme par le passé, demeurer entièrement soumises à la loi sur la transparence.

2.5.2 Révision de l'ordonnance sur l'accréditation et la désignation

Le projet de révision de l'ordonnance sur l'accréditation et la désignation (OAccD) contenait une norme selon laquelle les résultats des expertises et des contrôles effectués par le Service d'accréditation suisse (SAS) devaient demeurer confidentiels. Appelé à se prononcer à ce sujet dans le cadre de la consultation des offices, le préposé a attiré l'attention sur le fait que la réserve désignant certaines informations comme secrètes (y compris les informations confidentielles) doit être réglementée dans une loi fédérale, donc dans une loi au sens formel. Ce n'est que dans ce cas qu'il y a disposition spéciale au sens de l'art. 4 LTrans. La nouvelle norme sur la confidentialité serait réglementée uniquement dans une ordonnance, c'est-à-dire dans un texte légal au sens matériel, et non pas dans une loi fédérale. C'est pourquoi nous ne sommes pas dans le cas d'une disposition spéciale et la loi sur la transparence continue d'être applicable aux rapports du SAS.

3. Le PFPDT

3.1 Migration vers Windows 7 et système de gestion des affaires GEVER

Nous avons reçu cette année de nouveaux postes de travail sous Windows 7. Cette migration matérielle et logicielle constitue une occasion pour réévaluer les besoins réels en matière de solutions informatiques, à commencer par notre propre système de gestion des affaires. Nos exigences en matière de confidentialité des données n'étant cependant pas satisfaites, nous avons été contraints de porter notre système EDÖB-Office dans le nouvel environnement Windows 7, où il subsistera jusqu'à ce qu'une solution équivalente soit disponible.

Comme la majorité des offices de la Confédération, nous recevons cette année de nouveaux postes de travail sous Windows 7. Cette migration matérielle et logicielle requiert une planification de projet et constitue une occasion pour réévaluer les besoins réels en matière de solutions informatiques, à commencer par notre propre système de gestion des affaires. Bon nombre d'utilitaires aujourd'hui plus vraiment utiles ou utilisés ont ainsi pu être supprimés. Quelques autres applications seront par contre réinstallées dans leur version portable, afin d'éviter les importants délais de mise à jour qui pourraient finir par nuire à la sécurité globale (failles non corrigées, nouvelles fonctions non disponibles), de même que les frais non négligeables que la paquetisation de tels logiciels par le prestataire de services aurait engendrés.

Afin de préparer notre migration vers un produit GEVER standard, nous avons fait agréer notre nouveau système de classement par les Archives fédérales suisses, tandis que nos directives d'organisation font l'objet d'une actualisation régulière depuis leur introduction en 2000 déjà. Nos exigences en matière de confidentialité des données n´étant cependant pas encore satisfaites par les systèmes homologués, nous avons été contraints de porter notre propre système EDÖB-Office dans le nouvel environnement Windows 7 (principales adaptations liées à MS-Office 2007 Professional et PGP Version 10), où il subsistera jusqu´à ce qu´une solution équivalente soit disponible. Rappelons ici que grâce au chiffrement des contenus assuré par l'environnement PGP, notre système EDÖB-Office garantit la haute confidentialité des documents à l'égard des administrateurs internes (application et base de données), des différentes tâches internes (direction d'office, protection des données, droit d'accès indirect, transparence) et surtout du prestataire externe de solutions (postes de travail, réseau, imprimantes, fichiers, messages, base de données, sauvegardes, etc.) qu'est actuellement l'OFIT.

3.2 Sixième journée de la protection des données

La Journée de la protection des données était axée cette année sur les thèmes «Traitement des données par les entreprises» et «Utilisation des nouveaux médias par les jeunes». Pour les deux domaines, des supports de sensibilisation au développement desquels nous avons contribué ont été présentés au public.

À l'ère du tout numérique, les responsables des banques de données d'entreprises ou d´organisations sont amenés à traiter des quantités considérables de données personnelles, relatives notamment aux collaborateurs et aux clients. Lors du traitement de ces données, ils doivent tenir compte d'un certain nombre d'exigences légales et techniques, ce qui peut présenter des difficultés, en particulier pour les PME. Lancé à l'occasion de la sixième Journée de la protection des données du 27 janvier 2012, le nouveau service en ligne interactif «ThinkData» a pour objectif d'aider entreprises, organisations, autorités et particuliers en les sensibilisant aux exigences légales applicables au traitement des données personnelles et à la nécessité de créer la transparence. Le site www.thinkdata.ch propose ainsi des informations et des conseils adaptés aux besoins de chacun, dans de nombreux domaines tant juridiques que technologiques.

Le projet ThinkData à but non lucratif est issu d'une réflexion associant l'autorité de protection des données du Canton de Genève, l'Université de Genève, l'Institut de hautes études en administration publique (IDHEAP) de Lausanne, l'Observatoire technologique de Genève, le PFPDT et plusieurs autres acteurs. Le service n'est disponible pour l'instant qu'en langue française mais le sera bientôt en langue allemande. Par ailleurs, le Préposé a publié un matériel d'enseignement sur les précautions élémentaires à prendre pour sécuriser les données. Destiné aux jeunes adultes friands de nouveaux médias, il propose des informations et conseils pour protéger leurs données lorsqu'ils utilisent les nouveaux médias. Il aborde des thèmes tels que les réseaux sociaux, les communications mobiles et les portails en ligne. Les enseignants sont invités à utiliser en classe ce dossier éducatif complet organisé en neuf leçons, indépendantes les unes des autres. Il est disponible pour toutes les parties intéressées sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet – Enfants et adolescents – Matériel d'enseignement scolaire pour les 16-19 ans (en allemand; les versions française et italienne sont prévues pour l'automne 2012).

3.3 Publications du PFPDT au cours de l'année sous revue

Les citoyens et citoyennes trouveront sur notre site web des informations relatives à nos activités dans les domaines de la protection des données et du principe de la transparence. Durant l'exercice en cours, nous avons entre autres mis en ligne des explications concernant l'informatique en nuage, la directive «Vie privée et communications électroniques» de l'UE ainsi qu'un matériel d'enseignement sur les principes de base de la sécurité des données.

De plus en plus d´entreprises, d´autorités et d´institutions confient à des entreprises externes le traitement de leurs données effectué jusqu´ici en interne, et misent ainsi sur l´informatique en nuage (cloud computing). Notre document à ce sujet expose les dangers que l´informatique en nuage recèle pour la sphère privée et donne des recommandations sur la protection des données. Ce document se trouve sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données– Entreprises.

Nous avons également publié des explications sur la directive «Vie privée et communications électroniques» de l'UE pour davantage de transparence sur Internet. À la fin de 2009, le parlement de l'UE a arrêté une révision de cette directive afin de tenir compte des défis que présentent les technologies numériques. Le but est d'améliorer la transparence et la sécurité au profit des utilisateurs. Nos explications abordent entre autres l'application des dispositions contenues dans la directive et montrent quelles sont les conséquences possibles pour la Suisse. Les explications se trouvent sous la rubrique Thèmes – Protection des données – Entreprises (cf. aussi ch. 1.3.2 du présent rapport d'activités).

La version révisée de notre «Guide relatif aux mesures techniques et organisationnelles de la protection des données» donne une introduction aux dangers que présentent les systèmes modernes d'information sous l'angle de la protection des données. Ce guide a été conçu comme une aide à la mise en œuvre de mesures adéquates dans le but d'assurer une protection optimale et appropriée des données personnelles. Les thèmes principaux de la protection des données y sont présentés sous l'angle des mesures techniques et organisationnelles à mettre en place, comme le chiffrement, l'anonymisation et l'authentification.

Dans le domaine de la vidéosurveillance effectuée par des particuliers, nous avons revu le feuillet thématique existant et publié un nouveau feuillet sur la vidéosurveillance de l'espace public (cf. Documentation – Protection des données – Feuillets thématiques – Vidéosurveillance; voir aussi ch. 1.2.6 du présent rapport d'activités).

Dans le domaine de la sécurité des données, nous avons publié un matériel d'enseignement sur les précautions élémentaires à prendre pour sécuriser les données. Destiné aux jeunes adultes friands de nouveaux médias, il propose des informations et conseils pour protéger leurs données lorsqu'ils utilisent les nouveaux médias (voir ch. 3.4 du présent rapport d'activités). Les documents mentionnés peuvent être téléchargés de notre site web www.leprepose.ch, sous Thèmes – Protection des données – Internet – Enfants et adolescents – Matériel d'enseignement scolaire pour les 16-19 ans.

3.4 Matériel d´enseignement pour les jeunes adultes

La sensibilisation des jeunes à l'usage qu'ils font de leurs données personnelles a également été une des principales activités de cette année dans le domaine de la formation et de la sensibilisation. Pour donner aux jeunes adultes les connaissances nécessaires en matière de sécurité des données lors de l'utilisation des nouveaux médias, nous avons conçu un matériel d'enseignement qui peut être téléchargé gratuitement en ligne. Les enseignants alémaniques peuvent utiliser ces leçons pour leur enseignement depuis janvier 2012.

Des études récentes, telles que l´étude JAMES effectuée en 2010 par la Haute école des sciences appliquées de Zurich ZHAW, montrent dans quelle mesure les jeunes d´aujourd´hui font usage des nouvelles technologies. Les réseaux sociaux, les jeux vidéo et les plateformes de jeux ou l´utilisation d´Internet depuis un téléphone portable occupent une place importante dans leur vie quotidienne. Ils sont cependant souvent laissés à eux-mêmes. Le soutien apporté par les parents et les éducateurs est, surtout pour les personnes de faible niveau d´éducation, souvent limité ou superficiel. C´est pourquoi les écoles jouent un rôle d´autant plus important dans l´enseignement des compétences en matière de médias. Pour aider les enseignants, nous avons lancé en 2010 un projet de formation en trois volets portant sur plusieurs années avec pour objectif de montrer aux enfants et aux adolescents comment utiliser les nouvelles technologies de manière sûre et raisonnable, tout en mettant l´accent sur la protection de leur vie privée (cf. notre 18e rapport d'activités 2010/2011, ch. 3.3 et 3. 4).

L'actuel matériel d'enseignement met l'accent sur la sécurité des données, c'est-à-dire sur l'approche à adopter pour protéger efficacement ses données personnelles, et donc sa sphère privée, dans les médias. Il s'adresse aux élèves de deuxième cycle du secondaire. Les contenus ont été développés en coopération avec l'agence kik, spécialisée dans la production de matériel pédagogique. Les enseignants sont invités à utiliser ce dossier éducatif complet organisé en neuf leçons, indépendantes les unes des autres, pour leur enseignement. Les sujets traités englobent entre autres les sites de réseautage social, les communications mobiles et les portails en ligne. En termes de contenu et de concept, ce matériel d'enseignement complète les offres existantes de sensibilisation.

Le matériel pédagogique, pour l'heure en allemand uniquement, est gratuitement disponible en téléchargement pour toute personne intéressée sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet – Enfants et adolescents. Les versions française et italienne sont prévues pour l'automne 2012.

3.5 Formation pour les étudiants de l'Université de Neuchâtel

À la demande du préposé cantonal neuchâtelois à la protection des données, nous avons élaboré un cours à l'intention des étudiants de niveau master de l'Université de Neuchâtel. Ce cours portait sur le travail du préposé fédéral à la protection des données et à la transparence et présentait, sous la forme d'un exemple concret, un cas de protection des données dans le domaine du travail traité par notre service.

Dans le cadre du séminaire dont il a la charge à l'Université de Neuchâtel, le préposé cantonal neuchâtelois, M. Christian Flückiger, a organisé une journée de cours à Berne, dans nos locaux. Il a souhaité que nous intervenions durant cette journée sous la forme d'un cours de deux heures environ, qui aborde le thème de la protection des données dans le domaine du travail sous les angles juridique et technique.

Nous avons divisé ce cours en plusieurs parties. Tout d'abord, nous avons présenté l'organisation de notre service et les deux axes principaux de notre travail: le conseil et la surveillance. Une présentation plus approfondie du processus de l'établissement des faits a permis aux étudiants de comprendre le mécanisme de surveillance. Ce thème a été illustré de manière concrète par la présentation d'un cas réel, traité par nos services. Finalement, nous avons donné aux étudiants un bref aperçu des technologies actuelles qui interviennent dans les questions de protection des données liées au monde du travail, comme par exemple, les systèmes de reconnaissance biométrique et les systèmes de géolocalisation.

Nous avons pu constater l'intérêt des étudiants pour le thème de la protection des données qui mêle étroitement des aspects techniques et juridiques.

3.6 Journée de protection des données au centre CEDIDAC

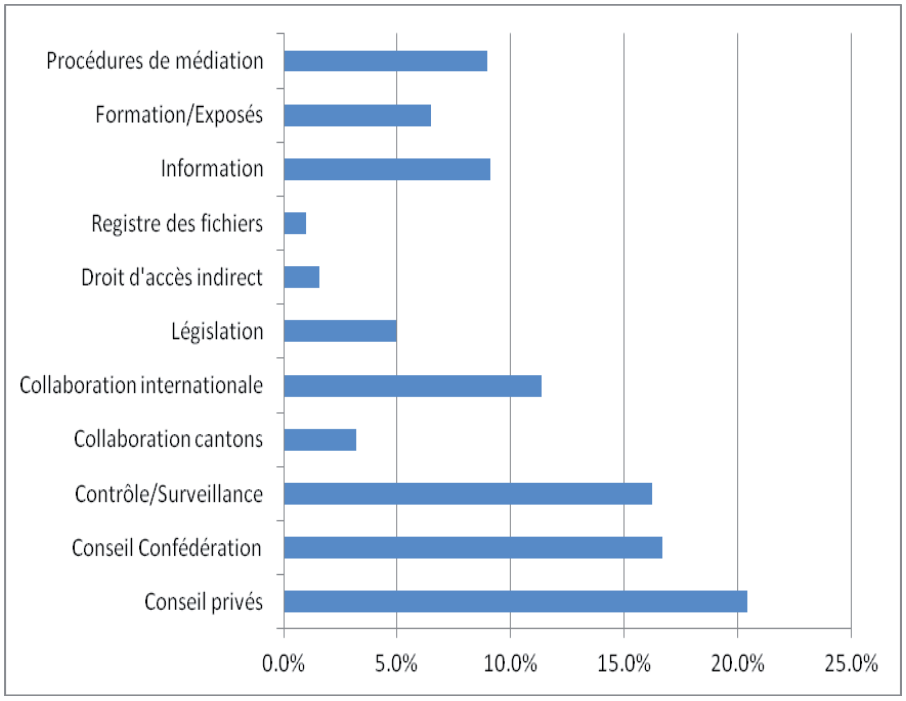
À la demande du Centre du droit d'entreprise CEDIDAC de l'Université de Lausanne, nous sommes intervenus lors de son colloque du 11 octobre 2011 en apportant des éclairages pratiques d'actualité. Cette demi-journée de formation était consacrée à quelques aspects choisis du droit de la protection des données.

Dans le cadre de sa demi-journée «Protection des données: Questions pratiques pour les entreprises et la rédaction des contrats» organisée conjointement avec le Master en droit, sécurité et criminalité des nouvelles technologies quatre thèmes importants ont été abordés sous un angle pratique. Le premier intervenant a abordé les aspects du traitement des données personnelles du travailleur; le deuxième a parlé de la protection des données dans les établissements bancaires, le troisième a décrit le cadre juridique applicable aux fichiers-clients et aux cartes fidélité et le quatrième a présenté les bonnes pratiques («best practices») en matières de politique de confidentialité. Plus d'une centaine d'avocats et de juristes d'entreprise de Suisse romande ont participé à cette manifestation.

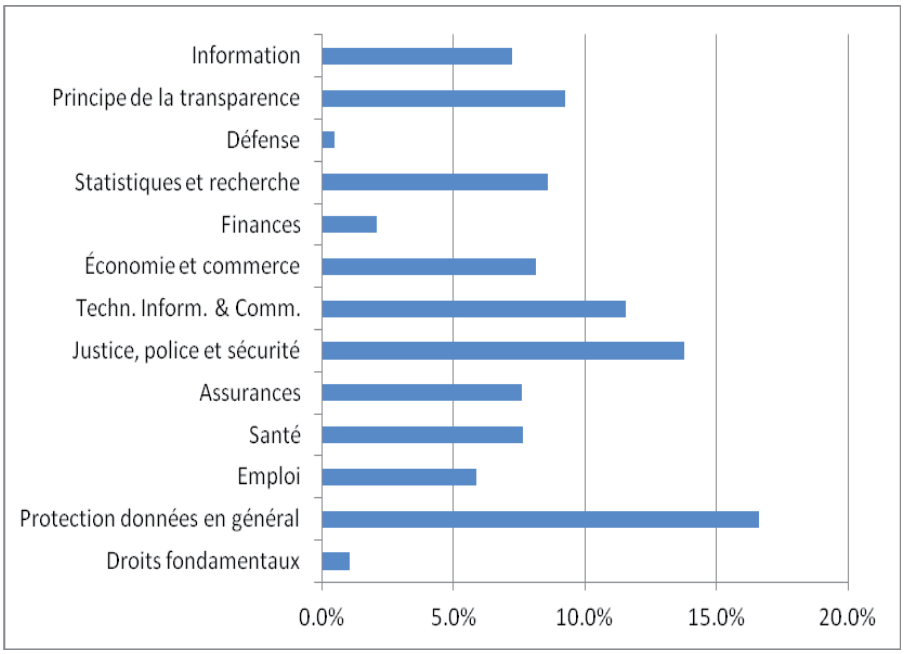
Pour clore cette journée thématique, nous avons donné une conférence intitulée «Pratique actuelle du Préposé fédéral à la protection des données et à la transparence». Nous avons divisé cette intervention en deux parties. Dans un premier temps, nous avons présenté l'organisation et le processus d'établissement des faits afin de permettre aux participants de mieux comprendre le mécanisme de surveillance prévu par la loi sur la protection des données. Dans un second temps, nous avons illustré notre travail en évoquant des cas réels traités par nos services. Ces éclairages sur notre fonctionnement et sur notre pratique ont été accueillis avec un grand intérêt.

3.7 Statistique des activités du PFPDT du 1er avril 2011 au 31 mars 2012

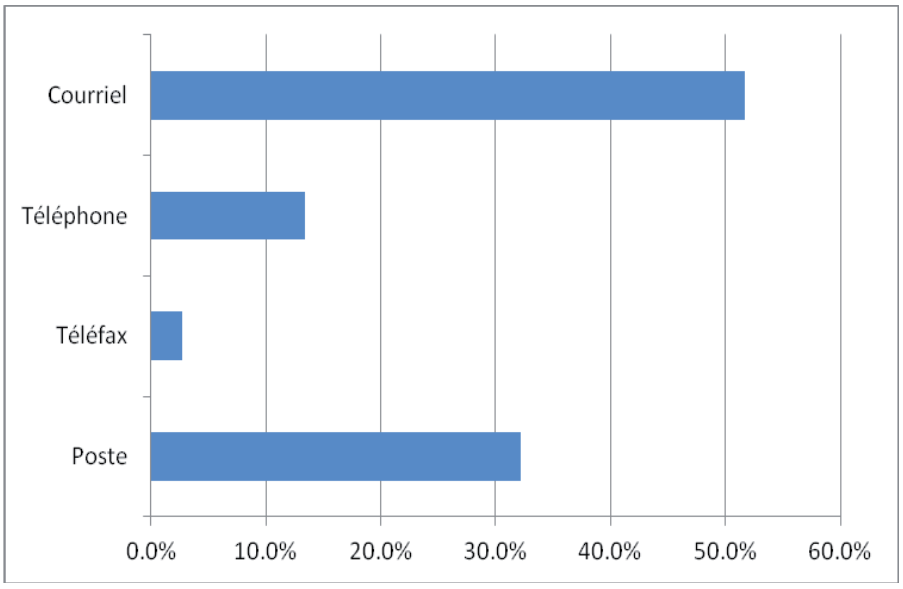
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.8 Statistique des demandes d´accès présentées auprès des départements en vertu de l´art. 6 de la loi sur la transparence (Période: 1er janvier 2011 au 31 décembre 2011)

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
ChF	24	15	3	6	0
DFAE	80	26	17	37	0
DFI	87	36	27	19	5
DFJP	51	25	10	16	0
DDPS	27	15	3	9	0
DFF	45	16	23	6	0
DFE	42	10	18	10	4
DETEC	110	60	25	25	0
Total 2011 (en %)	466 (100%)	203 (44%)	126 (27%)	128 (27%)	9 (2%)
Total 2010 (en %)	239 (100%)	106 (45%)	62 (26%)	63 (26%)	8 (3%)
Total 2009 (en %)	232 (100%)	124 (54%)	68 (29%)	40 (17%)	-
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

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
ChF	13	5	3	5	0
PFPDT	11	10	0	1	0
TOTAL	**24**	**15**	**3**	**6**	**0**

Département fédéral des affaires étrangères DFAE

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
DFAE	80	26	17	37	0
TOTAL	**80**	**26**	**17**	**37**	**0**

Département fédéral de l'intérieur DFI

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DFI	5	2	1	2	0
BFEG	0	0	0	0	0
OFC	7	5	1	0	1
AFS	4	2	2	0	0
Météo Suisse	1	1	0	0	0
BN	0	0	0	0	0
OFSP	33	16	6	10	1
OFS	0	0	0	0	0
OFAS	11	5	6	0	0
SER	1	1	0	0	0
Conseil des EPF	0	0	0	0	0
MNS	0	0	0	0	0
SWISS MEDIC	19	4	7	5	3
FNS	3	0	2	1	0
SUVA	3	0	2	1	0
TOTAL	**87**	**36**	**27**	**19**	**5**

Département fédéral de justice et police DFJP

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DFJP	5	2	1	2	0
OFJ	8	1	2	5	0
FEDPOL	4	3	0	1	0
METAS	1	0	1	0	0
ODM	15	10	2	3	0
ISDC	0	0	0	0	0
IPI	3	1	2	0	0
CFMJ	11	7	0	4	0
CAF	1	0	1	0	0
ASR	0	0	0	0	0
CSI	2	1	0	1	0
CNPT	1	0	1	0	0
TOTAL	**51**	**25**	**10**	**16**	**0**

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

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DDPS	16	10	0	6	0
Défense/ armée	5	1	2	2	0
SRC	1	0	1	0	0
armasuisse	2	1	0	1	0
OFPP	1	1	0	0	0
OFSPO	2	2	0	0	0
TOTAL	**27**	**15**	**3**	**9**	**0**

Département fédéral des finances DFF

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DFF	7	2	4	1	0
AFF	4	2	1	1	0
OFPER	3	2	1	0	0
AFC	4	2	2	0	0
AFD	2	2	0	0	0
RFA	0	0	0	0	0
OFCL	4	0	3	1	0
OFIT	1	0	0	1	0
CDF	19	6	11	2	0
SFI	0	0	0	0	0
PUBLICA	0	0	0	0	0
CC	1	0	1	0	0
TOTAL	**45**	**16**	**23**	**6**	**0**

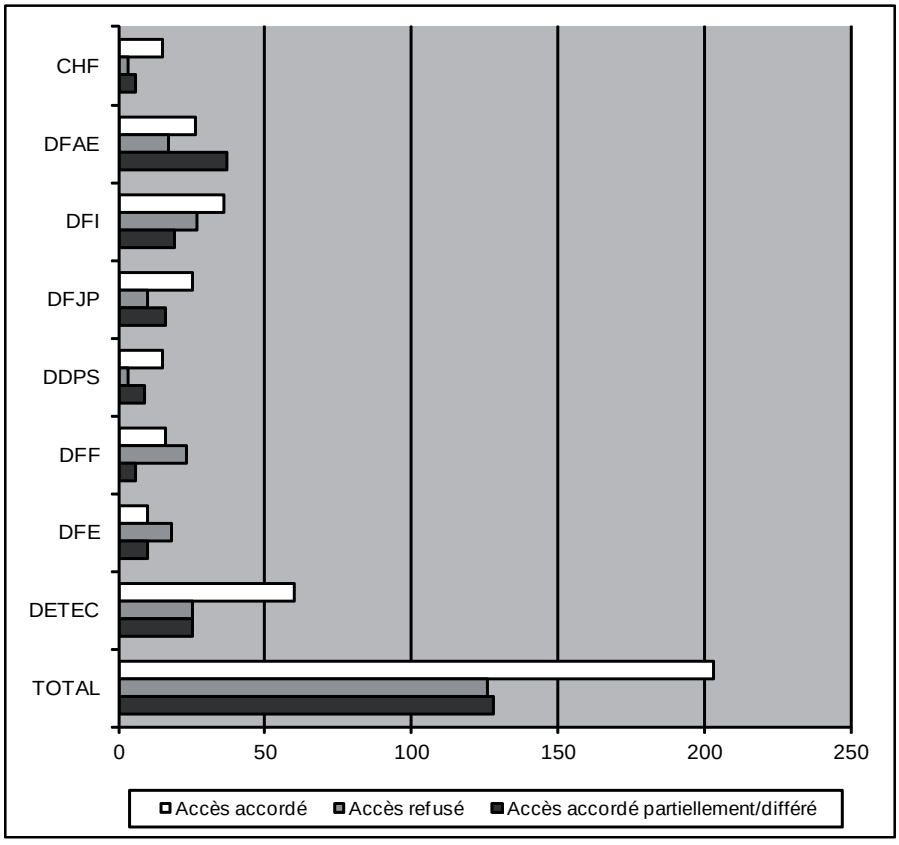
Département fédéral de l'économie DFE

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DFE	2	1	0	1	0
SECO	7	0	6	1	0
OFFT	2	1	1	0	0
OFAG	17	3	8	2	4
OVF	3	1	1	1	0
OFAE	1	1	0	0	0
OFL	5	3	0	2	0
SPr	2	0	2	0	0
COMCO	3	0	0	3	0
ZIVI	0	0	0	0	0
BFC	0	0	0	0	0
TOTAL	**42**	**10**	**18**	**10**	**4**

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

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SG DETEC	2	0	1	1	0
OFT	3	3	0	0	0
OFAC	19	10	6	3	0
OFEN	18	2	7	9	0
OFROU	5	5	0	0	0
OFCOM	6	4	0	2	0
OFEV	22	12	4	6	0
ARE	4	0	3	1	0
COMCOM	0	0	0	0	0
IFSN	22	15	4	3	0
PostReg	2	2	0	0	0
AIEP	7	7	0	0	0
TOTAL	**110**	**60**	**25**	**25**	**0**

Traitement des demandes d'accès



3.9 Statistique des demandes d'accès présentées auprès du Ministère public de la Confédération en vertu de l'art. 6 de la loi sur la transparence (Période: 1er janvier 2011 au 31 décembre 2011)

Ministère public de la Confédération MPC

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
MPC	3	2	1	0	0
TOTAL	**3**	**2**	**1**	**0**	**0**

3.10 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 2011 au 31 décembre 2011)

Services du Parlement SP

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment/ différé	Demande d'accès pendante
SP	1	1	0	0	0
TOTAL	**1**	**1**	**0**	**0**	**0**

3.11 Nombre de demandes de médiation par catégories de requérants (Période: 1er janvier 2011 au 31 décembre 2011)

Catégorie de requérants	2011
Médias	24
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	10
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	9
Entreprises	16
Avocats	6
Total	**65**

3.12 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, avocat
Suppléant:	Walter Jean-Philippe, Dr. iur.

Secrétariat:

Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité 1:	10 personnes
Unité 2:	12 personnes
Unité 3:	2 personnes
Chancellerie:	4 personnes