18e Rapport d'activités 2010/2011

Préposé fédéral à la protection
des données et à la transparence

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Rapport d'activités 2010/2011 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 2010 au 31 mars 2011.

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. 410.018.d/f

Table des matières

Avant-propos

Le triomphe de l'«esprit petit-bourgeois» à l'ère du numérique?

«Celui qui profite de l'offre intéressante que différentes entreprises proposent sur Internet ne doit pas abandonner son droit à la vie privée, comme l'on pose son manteau au vestiaire. Si avoir l'esprit petit-bourgeois à l'ère du numérique signifie revendiquer ce droit fondamental de nature libérale, alors nous acceptons d'être qualifiés de petits bourgeois bornés!» Tel était le commentaire que l'on pouvait lire dans la NZZ fin février 2011, juste avant l'audience devant le Tribunal administratif fédéral concernant Google Street View. Nous pouvons tout à fait partager ce commentaire.

D'aucuns ont parlé de protection des données digne de l'ère préhistorique et de croisade contre la modernité, simplement parce nous exigeons de Google le respect de nos lois et que nous n'acceptons pas qu'une entreprise d'envergure mondiale définisse elle-même les mesures que l'on est en droit d'attendre en matière de protection de la sphère privée. La procédure dans l'affaire Google Street View et le débat qui l'entoure ont fait des vagues en Suisse comme à l'étranger, ont suscité diverses réactions (il semble, selon les sondages, que les opinions soient assez exactement partagées) et ont exacerbé la discussion à propos de la protection de la personnalité à l'ère numérique. Le Tribunal administratif fédéral a largement suivi nos arguments. Le jugement n'était pas encore entré en force au moment de la clôture de rédaction de notre rapport d'activités. Mais grâce à l'exposé convaincant de ses motifs, il contribue en tout état de cause à clarifier de manière déterminante la question de la délimitation entre les intérêts économiques des fournisseurs de nouvelles applications en ligne et les intérêts des personnes concernées quant à la protection de leurs droits de la personnalité.

De façon plus générale, la question essentielle est de savoir si l'on peut demander des comptes en vertu des lois suisses à une entreprise qui traite aussi des données hors de Suisse lorsque des habitants de ce même pays sont lésés dans leurs droits. Google n'a pas cessé de nié cette compétence. Si cette conception juridique venait à s'imposer, les conséquences sur la protection de la personnalité seraient dramatiques. Pour les entreprises actives au niveau mondial, ce serait une invitation à déplacer leurs traitements de données vers des contrées où le niveau de protection des données est le plus bas. Cette question a récemment incité l'Union européenne à intervenir: Viviane Reding, commissaire européenne en charge de la justice, a déclaré que toute entreprise qui intervient sur le marché de l'UE ou tout produit en ligne qui s'adresse à des consommateurs de l'UE doit répondre aux règles de l'UE. Il devrait en être absolument de même pour la Suisse!

Outre cette question formelle, on doit aussi se demander si la protection de la sphère privée peut être confiée à un simple logiciel entièrement automatisé, même s'il est prouvé qu'il ne fonctionne pas sans faille? Ou peut-on exiger un contrôle manuel si cela permet d'écarter le risque sérieux de violation de la personnalité? Est-ce qu'à l'avenir, ce qui est réalisable en matière de protection des données dépendra de ce qu'un logiciel peut effectuer à un moment déterminé?

La procédure devant le Tribunal administratif fédéral a aussi dégagé les points faibles de la loi et de la coordination internationale. Ces points faibles peuvent-ils être éliminés et comment? Au niveau national, l'évaluation de l'efficacité de la loi sur la protection des données, demandée récemment par le Conseil fédéral, offrirait un point d'appui. Vers la fin de l'année, et sur la base de cette évaluation, le Conseil fédéral établira un rapport destiné au Parlement sur la nécessité d'optimiser la loi sur la protection des données. Entre temps, plusieurs interventions parlementaires ont requis une amélioration de la loi sur la protection des données.

De notre point de vue, la première question à laquelle il faudrait répondre au niveau législatif est de savoir si les produits et les services ayant un grand impact sur la sphère privée ne devraient pas être soumis, avant leur lancement, à un contrôle de conformité à la protection des données et si le fournisseur ne devrait pas apporter la preuve qu'il a entrepris tout ce que l'on pouvait attendre de lui afin de protéger les droits de la personnalité. Selon la situation juridique actuelle, la diffusion de ces produits ne peut être stoppée que lorsque la violation du droit a été constatée. Ce qui n'est pas plus judicieux qu'acceptable pour une entreprise novatrice qui investit beaucoup, et peut-être de façon incorrecte, dans le développement d'un produit, ni non plus pour les personnes concernées.

Indépendamment du jugement des tribunaux dans l'affaire Google Street View, la question de la compétence nationale demeure une question cruciale pour le Préposé fédéral à la protection des données. Que faire par exemple lorsque les fournisseurs de réseaux sociaux offrent à leurs utilisateurs des prestations de services qui affectent la sphère privée de tiers, qui n'ont ni été informés, ni ont donné leur accord? Qui est responsable? L'utilisateur, qui fait usage des offres et transmet au réseau des informations sur des tiers, ou le fournisseur lui-même? Et où porter plainte le cas échéant? Autant de questions en suspens, qui n'ont pas non plus encore vraiment trouvé de réponse au niveau international.

Une autre question se pose dans ce contexte: comment améliorer la coordination et la coopération internationale? L'un des arguments de Google est que la Suisse serait le seul pays au monde où un procès lui est fait pour violation de la protection des données, alors que dans plus de vingt autres pays, l'introduction de Street View a eu lieu

sans résistance. Même si ces affirmations étaient vraies, il n'en demeure pas moins que les exigences posées par Street View varient selon les pays. Ce qui permet bien sûr à une entreprise agile d'implanter ses produits en premier lieu dans les pays dans lesquels elle ne rencontrera que peu ou pas de résistance et ensuite de mettre les autres pays sous pression, en invoquant une situation de fait.

Les révélations et les activités de Wikileaks nous mettent face à des questions brûlantes. Une obligation illimitée de transparence doit-elle aussi protéger les «lanceurs d'alerte» lorsque les révélations (whistleblowing) menacent des personnes à tort? Dans quelle mesure sont-elles licites lorsqu'elles touchent à des secrets de fonction ou à des secrets d'affaires? Le vif débat public qui a accompagné ces révélations a permis de clarifier certains points. L'administration publique et l'économie doivent créer des conditions permettant de dénoncer les abus et anomalies constatés sans que l'auteur de cette alerte ne soit «mis au pilori». La Confédération a pris les devants et a établi des règles claires. Les administrations cantonales ont encore du pain sur la planche, de même que les milieux économiques à certains égards. On ne peut accepter que des innocents soient anonymement noircis. Un lanceur d'alerte doit entreprendre toutes les démarches que l'on est en droit d'attendre de lui, notamment informer les instances parlementaires, avant de porter le sujet dans l'arène publique.

Le cas Eberle a montré qu'un préposé à la transparence, qui est aussi préposé à la protection des données, est à même de procéder à une juste pondération entre l'intérêt du public à bénéficier d'une transparence maximale et l'intérêt d'un particulier à la protection de sa sphère privée. Un journaliste voulait consulter la convention de départ de l'ancien secrétaire général du conseiller fédéral Blocher, ce que le DFJP et le Tribunal administratif fédéral avaient refusé dans un premier temps, contrairement à notre recommandation. Suite au grief du Tribunal fédéral selon lequel l'instance inférieure n'avait pas procédé à une pesée des différents intérêts en jeu, le Tribunal administratif fédéral s'est finalement rangé à notre appréciation: dans le cas concret, les intérêts du public à la divulgation de l'indemnité de départ sont prépondérants.

Nous sommes – du moins semble-t-il – presque arrivés au but en ce qui concerne l'élimination du droit indirect d'accès aux données dans le domaine de la protection de l'État. Depuis mon entrée en fonction, il y a maintenant dix ans, je revendique régulièrement l'application générale du droit d'accès direct aux données dans le domaine de la protection de l'État. En d'autres termes, le demandeur doit généralement pouvoir consulter lui-même les dossiers demandés si les intérêts de la protection de l'État ne s'y opposent pas. Après le rejet par le Parlement en 2010 d'une intervention dans ce sens, le Conseil fédéral œuvre désormais, dans le cadre de la modification de la «LMSI réduite», pour que l'on introduise un droit de consultation direct conformément aux règles des art. 8 et 9 LPD. Nous avons le ferme espoir qu'après le rapport «Traitement

des données dans le système d'information relatif à la protection de l'État ISIS», élaboré par sa commission de surveillance (la Délégation des Commissions de gestion des Chambres fédérales, DélCdG), le législateur entende améliorer les droits des personnes concernées. Ce rapport a en effet permis de dégager de sérieuses lacunes dans le domaine de la protection de l'État et nous a valu un flot inhabituel de demandes d'accès. Afin de prendre en compte le sentiment d'insécurité ressenti par bon nombre de citoyens, nous avons fait tout notre possible pour traiter ces demandes en priorité et l'ensemble des demandes ont pu être traitées à la fin de l'année dernière. En raison du caractère spécial de la situation, nous avons fait usage dans de nombreux cas de la disposition d'exception prévue à l'art. 18 LMSI et avons informé les demandeurs qu'ils n'étaient pas enregistrés.

Enfin, la sensibilisation des enfants et des jeunes a également été un thème majeur durant l'année écoulée. Pour nous, il s'agissait essentiellement de soutenir des initiatives privées. Les pouvoirs publics ne doivent pas être les seuls à sensibiliser la jeune génération à propos de l'impact des nouveaux médias sur la sphère privée. C'est donc avec grande satisfaction que nous avons suivi et soutenu cette initiative exemplaire qu'est la campagne multimédia «NetLa – mes données m'appartiennent». NetLa a été lancée par le Conseil pour la protection de la sphère privée et a été financée dans une large mesure par l'économie privée. En coopération avec le Conseil, nous avons présenté cette campagne au public à l'occasion de la 5e Journée européenne de la protection des données. Il était important à nos yeux que cette campagne ne soit pas seulement conçue comme une action ponctuelle, mais que ce thème soit traité sur une période assez longue, avec diverses offres en fonction des âges, et qu'à la fin, une évaluation soit effectuée.

Hanspeter Thür

Répertoire des abréviations

ACC	Autorité de contrôle commune Schengen
AFAPDP	Association francophone des autorités de protection des données
CC	Code civil
CCT	Convention collective de travail
CDI	Convention de double imposition
CFV	Commission fédérale pour les vaccinations
ChF	Chancellerie fédérale
CP	Code pénal suisse
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
FABER	Registre automatisé des autorisations de conduire
fedpol	Office fédéral de la police
GEWA	Système de traitement des données en matière de lutte contre le blanchiment d'argent
IDE	Numéro d'identification des entreprises
ISAS	Système d'information sécurité extérieure
ISIS	Système d'information sécurité intérieure
JANUS	Système informatisé commun des Offices centraux de police criminelle de la Confédération
SUVA	Caisse nationale suisse d'assurance en cas d'accidents

LArm	Loi fédérale sur les armes, les accessoires d'armes et les munitions
LAsi	Loi fédérale sur l'asile
LAVS	Loi fédérale sur l'assurance-vieillesse et survivants
LCR	Loi fédérale sur la circulation routière
LDA	Loi fédérale sur le droit d'auteur et les droits voisins
LEIS	Loi fédérale sur l'échange d'informations entre les autorités de poursuite pénale de la Confédération et celles des autres États Schengen
LEp	Loi fédérale sur les épidémies
LEtr	Loi fédérale sur les étrangers
LFRC	Loi fédérale sur le renseignement civil
LIDE	Loi fédérale sur le numéro d'identification des entreprises
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOGA	Loi fédérale 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
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
LStup	Loi fédérale sur les stupéfiants et les substances psychotropes
LTrans	Loi fédérale sur le principe de la transparence dans l'administration
MOFIS	Registre automatisé des véhicules et des détenteurs de véhicules
N-SIS	Partie nationale du Système d'information Schengen
OAAE	Ordonnance sur l'acte authentique électronique
OCDE	Organisation de coopération et de développement économiques
OCPD	Ordonnance sur les certifications en matière de protection de données
ODM	Office fédéral des migrations

OFAC	Office fédéral de l'aviation civile
OFAG	Office fédéral de l'agriculture
OFAS	Office fédéral des assurances sociales
OFEV	Office fédéral de l'environnement
OFJ	Office fédéral de la justice
OFROU	Office fédéral des routes
OFS	Office fédéral de la statistique
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
OFIT	Office fédéral de l'informatique et de la télécommunication
OFPER	Office fédéral du personnel
OVid-TP	Ordonnance sur la vidéosurveillance dans les transports publics
PFPDT	Préposé fédéral à la protection des données et à la transparence
PNR	Passenger Name Records, Données des passagers aériens
RFID	Radio Frequency Identification
SAS	Service d'accréditation suisse
SER	Secrétariat d'État à l'éducation et à la recherche
SIPA	Système d'information sur le personnel de l'armée
SIS	Système d'information Schengen
SRC	Service de renseignement de la Confédération
SYMIC	Système d'information central sur la migration
TAF	Tribunal administratif fédéral
TF	Tribunal fédéral
TARGA	Registre automatisé des types de véhicules

1. Protection des données

1.1 Droits fondamentaux

1.1.1 Externalisation (Outsourcing) dans le cadre du recensement de la population

Dans le cadre du recensement de la population, nous avons contrôlé un institut privé qui traite des données sur mandat de l'Office fédéral de la statistique (OFS). Nous avons constaté d'une manière générale que les parties impliquées s'engagent à appliquer les prescriptions de protection des données. Ce contrôle n'est pas encore terminé.

L'OFS délègue le plus souvent la collecte des données nécessaires à ses enquêtes à des prestataires externes. Cette délégation à des tiers présente des risques particuliers du point de vue de la protection des données. C'est pourquoi nous avons procédé, dans le cadre du recensement de la population, à un contrôle des traitements de données qu'une entreprise privée d'étude de marché a effectués sur mandat de l'OFS lors de l'enquête Omnibus 2010. Les statistiques Omnibus font partie du recensement de la population et fournissent des informations complémentaires sur des sujets d'actualité. Dans le cas d'espèce, l'enquête auprès de la population suisse a porté sur les technologies de l'information et des communications et sur l'utilisation d'Internet. L'institut en question effectue régulièrement des enquêtes pour le compte de l'OFS. Le but de notre contrôle était d'identifier d'éventuels potentiels d'optimisation.

Nous avons, sur la base des documents reçus, vérifié les diverses étapes du traitement de données de leur collecte jusqu'à leur destruction. Nous avons porté une attention particulière d'une part au respect des exigences en matière de sécurité des données et à la séparation des diverses enquêtes, d'autre part aux mesures d'assurance qualité. Nous nous sommes également rendus sur place et avons demandé que l'on nous présente certains traitements de données.

Nous avons constaté que les parties impliquées sont sensibilisées aux aspects de la protection des données et qu'elles s'engagent à respecter les prescriptions légales applicables. Parmi les propositions d'optimisation que nous avons faites, quelques-unes ont été acceptées et appliquées par les parties, par exemple celles concernant la séparation des diverses enquêtes et le chiffrement symétrique des sauvegardes.

Aucune entente n'a encore pu être trouvée pour deux des points que nous avons critiqués. D'une part, nous avons constaté que l'OFS pouvait encore améliorer l'information préalable des personnes concernées. Jusqu'à ce jour, les personnes interrogées n'ont pas été informées explicitement de l'existence d'une obligation de donner des

renseignements. Un essai effectué par l'OFS, dans lequel les personnes interrogées avaient été informées du caractère facultatif de la participation avait donné un taux de réponse insatisfaisant. Pour l'enquête Omnibus 2011, l'OFS testera diverses manières d'informer. Ainsi, notre contrôle ne pourra être clos qu'après analyse de ces tests, soit vraisemblablement vers la fin de l'été 2011.

D'autre part, nous avons critiqué le contrôle qualité effectué par l'institut privé. Pour la majeure partie des enquêtes, l'institut emploie des personnes à temps partiel et non à plein temps. Celles-ci doivent être soigneusement formées car les questions posées lors de ces enquêtes sont exigeantes. Une des mesures d'assurance qualité prises par l'institut consiste à surveiller ses collaborateurs; ceux-ci sont informés d'une telle surveillance et donnent leur consentement au moment de leur engagement. Au cours des interviews, les personnes chargées de la surveillance peuvent à tout moment suivre discrètement la conversation téléphonique et voir également le formulaire de saisie sur l'ordinateur du collaborateur ainsi que les données qu'il introduit. Les personnes interrogées de même que les collaborateurs sont informés à chaque entretien que des tiers peuvent suivre la conversation. Les collaborateurs qui ont été contrôlés reçoivent à la fin de leur travail une analyse du contrôle effectué sur laquelle ils doivent prendre position avant de pouvoir quitter leur place de travail.

Nous considérons ce genre de contrôle de qualité comme disproportionné, car il donne l'impression aux collaborateurs d'être sous surveillance constante, même si seule une petite partie des conversations sont effectivement contrôlées. Étant donné que ce genre de contrôle représente une atteinte sérieuse à la sphère privée, nous sommes d'avis que les collaborateurs doivent être informés explicitement avant chaque contrôle que leur conversation va être mise sur écoute. De même, les conséquences possibles des évaluations des contrôles doivent être définies de manière systématique et claire pour les collaborateurs.

1.1.2 Recensement 2010: microrecensement mobilité et transports

Un certain nombre de citoyens et citoyennes se sont plaints de l'envergure de ce microrecensement dont ils ont perçu les questions comme une atteinte disproportionnée à leur sphère privée.

Pour le microrecensement mobilité et transports, environ 60'000 ménages ont été interrogés. Ce microrecensement fait partie du recensement de la population. Les personnes concernées sont interrogées par téléphone avec l'assistance d'un ordinateur. Nous avons reçu diverses plaintes de la population, principalement concernant

l'obligation de renseigner, mais également concernant l'ampleur des questions. Dans le cadre de notre activité de conseil, nous avons attiré l'attention sur les conditions-cadre de cette enquête, notamment sur le fait qu'il n'est pas obligatoire d'y participer.

1.1.3 Projet de modernisation de la statistique de la formation

Le nouveau numéro AVS est la pièce essentielle du projet de modernisation de la statistique de la formation de l'Office fédéral de la statistique (OFS). L'utilisation de ce numéro nécessite une base légale claire.

L'OFS a entamé toute une série de projets de modernisation dont celui de la statistique de la formation. Ce dernier vise notamment à améliorer la comparabilité et l'actualité des données, à en augmenter la qualité, ainsi qu'à simplifier et à accélérer les processus de la saisie et du traitement des données. Pour atteindre cet objectif, l'OFS utilise de manière conséquente les données administratives des registres existants de la Confédération, des cantons et des écoles. Le nouveau numéro AVS à 13 positions (NAVS13), pièce essentielle de la modernisation, a été introduit comme identificateur des personnes commun à tous les registres. Au cours de l'année écoulée, nous avons reçu plusieurs demandes d'institutions de formation et d'écoles étonnées et préoccupées par cette pratique. Nous avons dès lors effectué un premier examen sommaire.

Pour qu'une utilisation générale du NAVS13 comme identificateur de personne soit possible, elle doit reposer sur une base légale formelle. Le cadre juridique sur lequel se base l'OFS étant peu clair en raison de l'interaction entre les diverses législations sur l'assurance vieillesse et survivants, sur l'harmonisation des registres et sur la statistique, nous avons décidé de procéder à un examen plus approfondi de cette question non seulement pour les statistiques de la formation, mais également dans le cadre des différents autres relevés et enquêtes statistiques.

1.1.4 Cycle de vie des données dans le cadre du numéro d'identification des entreprises

Le mot «radier» n'est pas toujours compris comme «supprimer définitivement». Nous en avons une nouvelle fois fait l'expérience dans le cadre de la consultation des offices pour l'ordonnance sur le numéro d'identification des entreprises (IDE). Dans nos prises de position, nous avons recommandé de régler les radiations dans le registre IDE de manière plus claire sur le plan légal.

Nous avons déjà à plusieurs reprises fait part de nos remarques critiques concernant l'introduction de l'IDE, principalement dans le domaine «Business to Business»

(B2B). Nous renvoyons à ce sujet aux déclarations faites dans nos précédents rapports d'activités.

Lors de la deuxième consultation des offices, nous avons attiré l'attention de l'Office fédéral de la statistique (OFS) sur le fait que l'ordonnance ne réglait pas toutes les étapes du traitement. La loi fédérale sur le numéro d'identification des entreprises (LIDE) règle bien la radiation des données IDE au niveau de la loi. Le problème est que le terme «radiation» est trompeur parce que les données ne sont en fait pas radiées (donc détruites), mais simplement marquées comme étant radiées. Les données sont ensuite encore publiées sur Internet pour une durée de dix ans. Le message relatif à la loi précise en plus que les services IDE ont encore accès à ces données après expiration du délai de dix ans.

Le principe de la proportionnalité exige que les données qui ne sont plus utilisées soient détruites, c'est-à-dire supprimées de manière irrévocable. Les bases légales susmentionnées ne règlent cette dernière étape du traitement que de manière insuffisante. De plus, il y a aussi des raisons concrètes qui s'opposent à l'utilisation du terme «radiation» dans ce domaine, car il est prévu que le numéro d'identification des entreprises remplace à moyen terme tous les autres numéros administratifs. À titre d'exemple, le numéro du registre du commerce n'est en fait jamais supprimé, les données concernant une entreprise restant indéfiniment accessibles dans le registre du commerce.

Nous avons donc demandé que la radiation dans le registre IDE soit réglée de manière claire et transparente dans les bases légales. L'OFS a finalement satisfait à notre demande.

1.1.5 Évolution de la certification de produits et de services

Suite aux difficultés rencontrées dans le domaine de la certification de produits et de services, nous avons décidé de geler provisoirement nos activités respectives et avons demandé à l'Office fédéral de la justice de clarifier certaines questions législatives.

Des représentants d'organes fédéraux et cantonaux, ainsi que de diverses entreprises privées actives dans les domaines de l'informatique, de la finance et de la santé, de la certification et de l'accréditation, se sont réunis au printemps 2010 pour faire le point sur la certification de produits et de services. Le groupe de travail est arrivé à la conclusion qu'une certification de produits (matériels/logiciels) informatiques, basée par exemple sur le catalogue d'exigences «European Privacy Seal» (EuroPriSe), n'était – sur le plan financier – guère envisageable dans un petit marché comme le nôtre et qu'elle présentait par ailleurs divers obstacles techniques et juridiques. En outre, plusieurs participants ont formulé le besoin d'introduire une certification des

services impliquant un traitement de données personnelles. Du point de vue technique, une telle certification serait sans autre réalisable, par exemple en étendant la norme ISO/CEI 20000 pour la gestion des services à la protection des données, à l'instar de la certification des organisations qui a été réalisée avec succès sur la base d'ISO/CEI 27001. Du point de vue juridique toutefois, la certification des services met en présence le mandant ou bénéficiaire de service, qui est en principe maître de fichier, et le mandataire ou prestataire de service, qui est un tiers au sens de l'article 10a alinéa 2 de la loi fédérale sur la protection des données (LPD). Selon cette disposition, le mandant doit en particulier s'assurer que le tiers garantit la sécurité des données, ce qui peut être interprété comme une invitation à la certification du tiers en matière de sécurité de l'information (ISO/CEI 27001). Le mandant étant cependant responsable du respect des principes de protection des données (éventuellement par le biais d'une certification organisationnelle), une certification en matière de protection des données est difficilement envisageable pour le prestataire de service.

Force est aussi de constater que la législation actuelle comporte des lacunes ou des imprécisions: l'art. 11 al. 1 LPD ne prévoit que la certification des systèmes et non celle des services; l'art. 5 de l'ordonnance sur les certifications en matière de protection des données (OCPD) qui règle la certification de produits pourrait être remplacé ou complété par une nouvelle disposition portant sur la certification de services. L'art. 11 al. 2 LPD dispose quant à lui que le Conseil fédéral édicte des dispositions sur l'introduction d'un label de qualité de protection des données, mais aucune prescription n'a été prévue dans l'ordonnance correspondante.

Face à ces problèmes et tenant compte du fait que nos pays voisins, comme l'Allemagne et la France, ont également des difficultés à mettre sur pied une certification des produits et/ou des services, nous avons décidé en été 2010 de geler nos travaux dans le domaine et avons prié l'Office fédéral de la justice de bien vouloir clarifier les questions législatives relatives à cette certification, le cas échéant dans le cadre de la révision de la LPD.

1.2 Protection des données – Questions d'ordre général

1.2.1 Via sicura

Le programme d'action de la Confédération visant à renforcer la sécurité routière révèle plusieurs points faibles au niveau de la protection des données. Nous avons proposé des améliorations, principalement dans les domaines de l'anonymisation, de la communication des données et des enregistrements des boîtes noires.

Nous avons eu la possibilité de prendre position sur Via Sicura, le programme d'action de la Confédération visant à renforcer la sécurité routière et sur le projet de révision de la loi fédérale sur la circulation routière (LCR). Plusieurs points délicats du point de vue de la protection des données doivent être relevés.

La première étape du programme consiste à créer, avec la révision de la LCR, une base légale au sens formel pour le registre des accidents de la route. Une partie de ce registre est le registre d'analyse, qui doit permettre d'établir des statistiques (cf. ch. 1.2.5 de notre 17e rapport d'activité 2009/2010). Le projet de révision de la LCR règle non seulement la statistique des accidents de la route, mais également la statistique des contrôles de la circulation routière. Dans les deux cas, les données sont saisies dans les registres d'analyse sous forme pseudonymisée (moyennant un NIP). Grâce au NIP et au lien avec d'autres systèmes d'information de l'Office fédéral des routes (OFROU), il est possible d'accéder en tout temps aux données effectives de la personne concernée. C'est pourquoi nous sommes d'avis que les données ne doivent pas être saisies dans les registres d'analyse sous forme pseudonymisée, mais dès le début sous forme anonymisée. Il serait pour le moins important que les données pseudonymisées soient rapidement supprimées ou alors anonymisées.

Le projet de loi permet ainsi au Conseil fédéral de prévoir dans une ordonnance la possibilité donner aux assureurs RC des véhicules automobiles des renseignements sur les mesures administratives prises à l'égard des preneurs d'assurance. Le message stipule cependant expressément que ceci n'est pas nécessaire pour assurer la sécurité routière et licite que dans certains cas. Par ailleurs, le Conseil fédéral aimerait «en contrepartie» obtenir des assureurs les données relatives aux accidents afin de pouvoir établir des statistiques plus précises. Nous avons souligné que de telles contreparties, n'étaient pas admissibles; soit les conditions (en matière de protection des données) pour la communication de données sont remplies, soit elles ne le sont pas, dans quel cas une communication des données n'est pas licite.

De plus, la révision prévoit une consolidation formelle des systèmes d'information existants. En d'autres mots, il s'agit de réunir les quatre registres actuels MOFIS, FABER,

ADMAS et TARGA en une seule base de données relative à l'admission à la circulation. Cette modification a été introduite en dernière minute. Nous avons déploré que la consultation des offices ait eu lieu avec un délai raccourci et sans consultation externe. À notre avis, il aurait été important d'examiner encore une fois soigneusement ce projet pour s'assurer que les aspects importants de protection des données, tels que la finalité, l'accès, les catégories de données traitées, ou la procédure de consultation en ligne, des systèmes d'information respectifs restent effectivement identiques après la fusion des bases légales. La manière dont il était prévu d'effectuer cette fusion sur le plan technique n'était pas claire pour nous non plus. Était-il par exemple prévu de préserver les registres actuels sous forme de (sous-)registres du nouveau système? À notre avis, le rapport explicatif ou le message aurait dû apporter des précisions à ce sujet. Nous approuvons cependant que le fichier des admissions à la circulation ne soit pas public et que les données relatives aux détenteurs de véhicule et aux couvertures d'assurance ne puissent être communiquées à des tiers que sous certaines conditions.

Le message a d'ailleurs justement précisé que l'utilisation d'enregistreurs de données (boîtes noires) constituait une atteinte importante à la vie privée. C'est pour cette raison que nous avons approuvé la disposition légale explicite qui stipule que les enregistrements de la boîte noire doivent servir uniquement à vérifier la vitesse du véhicule. La question qui se posait dans ce contexte était de savoir si ceci nécessitait également d'enregistrer l'emplacement, ce qui permettrait de générer un profil des déplacements. L'ordonnance du Conseil fédéral devrait en tous les cas faire l'objet d'un examen minutieux afin de déterminer quelles informations sont nécessaires et appropriées pour atteindre l'objectif visé et pour quelle durée celles-ci peuvent être conservées.

En ce qui concerne l'examen sur l'aptitude à la conduite, nous avons défendu le point de vue que les offices cantonaux de l'AI ou les médecins ne doivent pas signaler les éventuelles inaptitudes directement au service des automobiles, mais d'abord à un organe médical.

Le programme d'action Via sicura va maintenant faire l'objet de débats au Parlement.

1.2.2 Traitement des données personnelles lors de contrôles de vitesse par tronçon

L'Office fédéral des routes (OFROU) a effectué des essais avec ce qu'on appelle le «contrôle de vitesse par tronçon» et nous a préalablement soumis son projet. Du point de vue de la protection des données, nous n'avons émis aucune objection contre ce type de contrôle.

Préalablement aux essais de contrôles de vitesse par tronçon (CVT) prévus sur les routes nationales, l'OFROU nous a fait parvenir des documents pour prise de position. Les emplacements choisis pour ces essais sont le tunnel d'Arisdorf (BL) sur l'A2 ainsi qu'un tronçon de l'A9 dans le canton de Vaud. Contrairement aux radars habituels, les installations CVT ne contrôlent pas le respect de la vitesse en un seul point, mais sur un tronçon d'une certaine longueur. Une première phase d'essai a servi à vérifier le bon fonctionnement des nouveaux appareils de mesure sans sanctionner les éventuels dépassements de vitesse.

Nous n'avons, du point de vue de la protection des données, aucune objection à formuler contre l'utilisation de ces systèmes CVT. Tous les véhicules sont certes photographiés aussi bien au début qu'à la fin du tronçon, mais uniquement depuis l'arrière; de plus, les données concernant les véhicules respectant la vitesse maximale autorisée sont ensuite détruites et ne sont pas transmises à des tiers ou comparées avec celles d'autres systèmes d'information. Les véhicules qui dépassent la vitesse prescrite sont par contre automatiquement photographiés depuis l'avant. Seules ces données sont ensuite transmises au service de police cantonale compétent pour sanctionner l'infraction.

1.2.3 Surveillance vidéo selon les lois fédérales sur les chemins de fer et sur le transport des voyageurs

Les versions révisées de la loi sur les chemins de fer et de la loi sur le transport des voyageurs contiennent chacune depuis le 1er janvier 2010 une base légale au sens formel pour la vidéosurveillance. Les activités au bénéfice d'une concession sont maintenant régies par la LPD.

Le 1er janvier 2010 a vu l'entrée en vigueur des versions révisées de la loi fédérale sur les chemins de fer et de la loi fédérale sur le transport des voyageurs. Les deux lois sont applicables aux entreprises qui sont au bénéfice d'une concession fédérale. Elles stipulent que les activités effectuées dans le cadre d'une concession sont régies par la LPD. Cela signifie donc que les lois cantonales de protection des données ne sont pas applicables pour ces domaines d'activité. Ces deux lois prévoient désormais une base légale expresse au sens formel pour la vidéosurveillance. Les détails sont réglés dans

l'ordonnance sur la vidéosurveillance dans les transports publics. Celle-ci prévoit que la vidéosurveillance dans le cadre de transports de voyageurs réguliers et de type commercial par voie ferrée, routière ou navigable est régie par les dispositions de la LPD et non pas par les lois cantonales de protection des données. Cela signifie que la vidéosurveillance dans les transports publics relève dorénavant de notre compétence et non plus de celle des autorités cantonales de protection des données.

Un autre article concernant la vidéosurveillance dans les transports publics se trouve au ch. 1.6.2 du présent rapport d'activités.

1.2.4 Systèmes d'accès biométriques au centre sportif KSS: clôture de la procédure

Suite à un jugement du Tribunal administratif fédéral, le centre sportif KSS a dû modifier le stockage centralisé de données biométriques, opéré dans le cadre du contrôle de l'accès au centre. Comme nous l'avons constaté lors d'une vérification ultérieure sur place, le KSS applique le jugement en conformité avec les principes de la protection des données.

Après le jugement rendu par le Tribunal administratif fédéral le 4 août 2009, qui a qualifié le stockage centralisé de données biométriques, opéré dans le cadre du contrôle d'accès à un centre de sport et de détente, d'atteinte disproportionnée à la personnalité des clients (cf. notre 17e rapport d'activités 2009/2010, ch. 1.2.2), le Centre sportif KSS a entrepris la modification de son système d'accès. Les données biométriques seront à l'avenir certes toujours stockées de manière centralisée; le lien avec d'autres données personnelles relevées par le Centre sportif KSS a toutefois été éliminé et ne peut être établi qu'à l'aide de la carte d'abonnement. Celle-ci est en possession du client. Les données dérivées stockées de manière centralisée (templates ou données biométriques brutes stockées sous forme codée), font l'objet d'un cryptage dynamique. Leur décryptage n'est possible qu'à l'aide de la carte d'abonnement car une partie de la clé est enregistrée sur cette carte.

Un code stocké sur la carte permet de rattacher les données biométriques à d'autres données personnelles (identité et autres données d'utilisateur). Ce n'est que lorsque le client introduit sa carte dans l'appareil de lecture que, grâce au code d'attribution enregistré sur la carte, le modèle (template) d'empreintes digitales appartenant au client peut être chargé, décrypté et comparé avec l'empreinte digitale lue dans l'appareil. En outre, ce n'est qu'à ce moment que le rattachement aux données du client et de l'abonnement peut être effectué. Dès que la carte est retirée de l'appareil de lecture, la relation entre les blocs de données individuels est à nouveau interrompue et ne peut plus être rétablie par le Centre sportif KSS par un autre biais (par ex. par horodatage).

Ainsi, en théorie, le modèle peut certes être toujours rattaché à une personne car il constitue lui-même une donnée personnelle. Mais dans les faits, en l'état actuel de la technique, on ne peut procéder à ce rattachement sans la carte d'abonnement. Grâce au procédé décrit plus haut, les clients doivent autoriser de manière explicite et délibérée toute utilisation de leurs données biométriques et en gardent ainsi un contrôle maximum. Le Centre sportif KSS ne peut accéder aux données biométriques de personnes déterminées, ce qui est comparable à un stockage décentralisé des données.

Nous avons contrôlé ce nouveau système et avons constaté que les modèles d'empreintes digitales sont désormais séparés des autres données personnelles, comme nous l'avons décrit plus haut. En outre, tous les clients ont la possibilité d'acquérir une carte permanente exempte de toute donnée biométrique stockée de manière centralisée. Cette carte contient une photographie du visage du titulaire, ce qui permet au personnel à la caisse de l'identifier visuellement. Il n'y a aucun stockage centralisé des photos. Cette solution donne à chaque membre du centre sportif la possibilité soit d'autoriser le stockage centralisé de ses données biométriques, soit d'opter pour la solution (moins confortable) de la carte munie d'une photo d'identité.

Ainsi modifié, le nouveau système concrétise deux des points centraux du jugement du Tribunal administratif fédéral: d'une part, l'utilisation des données biométriques repose sur un consentement juridiquement valable puisque celui-ci ne peut être donné que librement. D'autre part, l'atteinte portée à la personnalité des intéressés par ce traitement de données est réduit au minimum. Nous sommes donc parvenus à la conclusion que le système d'accès biométrique du Centre sportif KSS est organisé en conformité avec les principes de la protection des données depuis la mise en œuvre complète de ces modifications.

Afin de pouvoir conserver une utilisation conviviale des bains, le Centre sportif va désormais introduire en continu le nouveau système: les cartes d'abonnement encore valables sont conservées; tous les nouveaux abonnements ou les abonnements prolongés seront commutés sur le nouveau système, de sorte que dans les deux années qui viennent, tous les abonnements seront modifiés.

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

Quelques personnes se sont plaintes des contrôles d'accès pratiqués dans de nombreuses stations de ski à l'aide de cartes d'abonnement comportant une photo. Nous examinons actuellement la conformité de ce système avec la protection des données.

En Suisse, la plupart des stations de ski utilisent des systèmes de contrôle des accès impliquant le stockage centralisé d'une photographie du visage, qui apparaît sur l'écran du personnel de contrôle à chaque passage du client au tourniquet. Étant donné qu'il n'y a pas de comparaison automatique entre la photo et la personne présente, on ne peut parler de systèmes de reconnaissance biométriques. Néanmoins, les photographies du visage sont des données brutes biométriques et comptent parmi les données personnelles sensibles qui, sont maintenant stockées de manière centralisée dans les stations de ski. Le traitement de ces données doit donc répondre à des exigences spécifiques, en particulier dans le domaine de la sécurité des données.

Afin de répondre aux préoccupations des titulaires d'abonnements qui nous ont contactés, nous avons décidé de soumettre ces systèmes de contrôle des accès à un examen en nous rendant dans l'une de ces stations. Notre analyse des informations rassemblées est en cours.

1.2.6 Système de reconnaissance biométrique pour la réservation d'espaces sportifs

Un club de tennis a introduit un nouveau système de réservation avec reconnaissance biométrique des personnes. Désormais, tout membre désireux de jouer sur un court doit procéder à la réservation de celui-ci à l'aide de son empreinte digitale. Informés par des membres du club inquiets de la situation, nous avons examiné de près ce système et avons constaté qu'il ne satisfaisait pas aux exigences de la protection des données et qu'il fallait donc le modifier. Nous avons élaboré une recommandation et nous examinons actuellement en collaboration avec le club comment la mettre en oeuvre.

Un club de tennis était régulièrement confronté au problème de l'occupation de ses courts par des personnes qui n'étaient pas autorisées à y jouer. La structure du club ne permet pas une bonne vue d'ensemble des installations et leur accès à partir de l'extérieur est mal protégé. De plus, le club ne possède pas de réception à proprement parler, de sorte qu'il est difficile de contrôler qui joue sur les courts. Un système de réservation

avec vérification par numéros personnels d'identification (NIP), introduit pour interdire l'accès aux personnes non autorisées, s'était révélé insuffisant, car ceux-ci avaient été illégalement transmis à des non-membres. Le club a donc décidé d'introduire un système qui vérifie le droit d'accès des joueurs à l'aide de leurs empreintes digitales. Les modèles (templates) d'empreintes digitales sont stockés de manière centralisée sur un ordinateur de sorte qu'il n'est pas nécessaire d'apporter sa carte de membre.

Informés par des membres du club, nous avons effectué un examen sur place et sommes parvenus au résultat suivant: l'utilisation de données biométriques afin de vérifier le droit d'accès est certes justifiée par un intérêt privé prépondérant. Mais il s'agit d'un système de vérification d'une installation sportive qui ne nécessite pas le stockage centralisé de données biométriques et qui, dès lors, est en principe disproportionné (cf. à ce propos nos considérations relatives au cas KSS dans notre 17e rapport d'activités 2009/2010, ch. 1.2.2). Les motifs avancés par le club en faveur de la centralisation des données (à savoir l'économie et le confort de ce système) ne suffisent pas pour justifier un traitement disproportionné des données. Nous en avons conclu que le club de tennis devait modifier son système de réservation.

Conformément à la recommandation que nous avons adressée au club, un certain nombre de possibilités lui sont offertes pour stocker les données de son système de vérification de l'utilisation des courts tout en respectant les exigences de la protection des données. La meilleure de ces possibilités consiste à stocker les données biométriques de manière totalement décentralisée sur un support de données qui est soumis au contrôle des personnes concernées elles-mêmes (par ex. sur la carte de membre). Une autre possibilité consiste à stocker les données biométriques de manière centralisée, mais de n'utiliser que des modèles et non pas des données brutes (comme les images d'empreintes digitales ou les photographies) et de crypter ces données avant le stockage. Les données doivent en outre être stockées séparément des autres informations personnelles (par ex. leur identité). Le lien avec une personne déterminée ne doit pouvoir être établi qu'avec le consentement délibéré et explicite de celle-ci, donné à l'aide d'une carte personnelle (cf. les considérations concernant la clôture de la procédure KSS, ch. 1.2.4 du présent rapport d'activités). Si l'on opte pour une solution sans carte, le stockage centralisé des données est inévitable. Mais il n'est autorisé que si aucune donnée brute n'est stockée et que si les caractéristiques biométriques utilisées ne laissent pas de traces physiques ou numériques (par ex. les veines des doigts ou le contour de la main, mais pas par ex. les empreintes digitales). Là aussi, les données doivent être stockées après avoir été cryptées et ne doivent pas avoir de lien avec d'autres données personnelles.

En outre, nous avons critiqué le fait que les mesures de sécurité des données ne sont pas du tout adaptées à la sensibilité des données biométriques. Ainsi, le serveur se trouve dans une pièce accessible de l'extérieur et protégée uniquement de manière rudimentaire contre l'effraction. De plus, la transmission des données est effectuée au moyen d'un réseau de radiocommunication (sans fil) qui est à la disposition de tous les membres pour l'accès à Internet dans l'enceinte du club. Ce système permettrait très facilement à des personnes non autorisées d'accéder physiquement et numériquement aux données en question. Or les données biométriques doivent faire l'objet d'une protection particulière. Nous avons donc recommandé au club d'augmenter la sécurité des données en prenant les mesures techniques appropriées. Pour cette raison, les autorisations d'accès et d'entrée des collaborateurs et des membres doivent être réglementées de manière précise et restrictive.

Nous examinons actuellement avec le club quelle variante de stockage des données pourrait être mise en œuvre et quelles sont les mesures concrètes d'ordre technique et organisationnel qui permettraient de garantir la sécurité des données.

1.2.7 Boîtes de nuit et centres pour la jeunesse: listes noires et biométrie

Divers établissements de divertissement nocturne ou centres de jeunes sont à la recherche de possibilités permettant de reconnaître les personnes frappées d'une interdiction d'entrée. Cette année, nous avons donc examiné plusieurs projets impliquant l'utilisation de systèmes de reconnaissance biométriques en vue d'identifier les délinquants figurant sur des listes noires. Du point de vue de la protection des données, l'aspect le plus problématique dans ce contexte est l'échange de données entre gérants d'établissements.

Les boîtes de nuit et centres de jeunes ont régulièrement des problèmes avec les personnes qui se font remarquer par leur consommation excessive d'alcool, par des actes de violence ou encore parce qu'ils ont commis des vols. Or il est difficile de faire respecter les interdictions d'entrée prononcées contre certains clients, car il n'est pas toujours possible de reconnaître ces personnes. En outre, les clients interdits d'entrée dans un établissement se tournent ensuite vers d'autres locaux où ils causent à nouveau des problèmes. Les gérants d'établissement sont donc à la recherche de solutions permettant de reconnaître les personnes indésirables à l'entrée même.

Les projets qui nous ont été remis pour examen présentent les modèles de base suivants: la personne interdite d'entrée est enregistrée dans une banque de données centralisée (liste noire) avec son identité, une photographie, ainsi que le motif et la durée

de l'interdiction. Une variante prévoit l'inscription de tous les clients de l'établissement dans la banque de données (système des clubs de membres), avec une mention spéciale pour les personnes interdites d'entrée. À l'entrée, toutes les personnes sont contrôlées soit par un simple contrôle visuel basé sur la carte de membre, soit par une caméra-vidéo avec reconnaissance automatique des visages. On peut donc reconnaître et éconduire dès l'entrée les personnes indésirables. Ces systèmes sont prévus pour être exploités en réseau. Tous les établissements raccordés pourraient ainsi accéder à toutes les données stockées dans la banque de données centrale. De cette manière, on pourrait aussi reconnaître les personnes qui se sont singularisés par leur comportement négatif dans d'autres établissements. Conformément à ce projet, les clubs de membres pourraient en outre utiliser et échanger les données à des fins de publicité ou dans le cadre de programmes de fidélisation.

Notre appréciation sous l'angle du droit de la protection des données est la suivante: De tels systèmes permettent de traiter et d'échanger des données personnelles (sensibles). Ceci doit être justifié par un intérêt privé prépondérant et les principes de protection des données, notamment le principe de la proportionnalité, doivent être appliqués. Le traitement de données personnelles n'est, dans ce contexte, pas problématique pour autant que l'on définisse exactement quand les données personnelles d'un individu sont saisies et qu'elles ne le soient que pour filtrer les entrées et dans l'intérêt de la sécurité.

Il en va autrement en cas d'échange des données entre les gérants des clubs en réseau. Là aussi, il faut qu'un intérêt privé prépondérant soit reconnu. C'est notamment le cas si l'on doit admettre, avec une relative certitude, qu'une personne va aussi mal se comporter en d'autres endroits. En cas de procédure d'appel automatisée et d'échange automatique des données entre les gérants d'établissement, on ne peut cependant vérifier s'il existe, dans le cas concret, un tel intérêt. Ainsi, seules les personnes pour lesquelles il existe objectivement un tel soupçon peuvent être introduites dans la banque de données; ce n'est en effet que dans ce cas que l'échange de données peut être justifié et que la transmission est proportionnée. Les visiteurs qui se voient interdire l'entrée d'un local en raison d'un conflit personnel avec le personnel du bar ou le gérant de l'établissement ne doivent par exemple pas être enregistrés dans la banque de données. Mais ainsi, la banque de données d'un club serait incomplète, ce qui reviendrait à compromettre fortement son objectif. Nous recommandons donc d'abandonner l'échange automatique de données et de ne transmettre les données que dans des cas justifiés.

L'enregistrement des données de tous les clients de l'établissement et leur utilisation à des fins de publicité ou dans le cadre de programme de fidélisation de la clientèle ne servent pas la sécurité et ne permettent pas non plus de filtrer les entrées. Ils sont

plutôt motivés par des intérêts purement économiques qui pèsent beaucoup moins lourd que la protection de la personnalité. La participation à des campagnes de publicité ou à des programmes de fidélisation de la clientèle doit donc être volontaire. Le consentement des personnes concernées devrait, le cas échéant, également porter explicitement sur un éventuel échange de données prévu entre les établissements.

Nous avons communiqué notre prise de position aux personnes concernées. Nous procéderons à un examen plus approfondi des projets dès que nous disposerons de leur planification détaillée.

1.2.8 Conformité du fréquencemètre avec la protection des données

Le fréquencemètre est un appareil qui sert à mesurer, sur la base d'une image vidéo, la fréquence avec laquelle des piétons ou des véhicules franchissent un certain endroit. Vu que, ce faisant, des personnes ou des objets pouvant être attribués à une personne déterminée sont enregistrés, il s'agit d'un traitement de données personnelles. Nous avons donc examiné le fréquencemètre sous l'angle de sa conformité avec les principes de la protection des données et sommes parvenus à la conclusion que les droits de la personnalité des individus concernés étaient respectés.

Le fréquencemètre se compose d'un mini-ordinateur personnel, d'une clé USB et d'une caméra-vidéo qui sont reliés les uns aux autres. La détermination des données de fréquence se fait par le biais de la caméra, sans stockage durable des photos. Un logiciel établit un œil électronique virtuel dans un secteur quelconque du champ de la caméra. Deux images-vidéo successives sont comparées en continu dans une mémoire électronique volatile. Si une modification d'image a lieu dans le secteur de l'œil électronique, ceci est identifié comme objet franchissant l'endroit en question. Cet élément est ensuite introduit dans une banque de données. Ensuite, les images-vidéo sont recouvertes par deux nouvelles images. Il n'y a pas de reconnaissance d'objet. Les données stockées dans la banque de données n'ont donc aucun lien avec des personnes.

Ce processus se répète 25 fois par seconde. Vu que les images-vidéo sont recouvertes en continu par d'autres images et qu'en fin de programme les deux dernières sont immédiatement effacées, chaque image n'est enregistrée que pendant quelques secondes. Cette durée extrêmement courte de stockage de données concernant potentiellement des personnes ne permet pas un traitement ultérieur de données personnelles.

Même si on peut reconnaître et parfois même identifier des personnes sur la photo produite par la caméra, nous estimons que l'intensité du traitement de ces données est réduite car la durée de stockage est extrêmement courte et il n'y a pas d'autre possibilité de traitement des données. Nous sommes d'avis que ce fréquencemètre ne constitue pas une atteinte illicite à la personnalité.

1.2.9 Communication de données AVS à des sociétés de gestion

La révision partielle de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS) doit permettre à la société de gestion des droits d'auteur ProLitteris d'obtenir des extraits du registre AVS pour lui permettre de percevoir les rémunérations de manière plus efficace.

En 2007, l'Institut fédéral de la propriété intellectuelle nous a contactés concernant une demande de ProLitteris visant à obtenir des données issues du registre AVS. Nous avons indiqué qu'une communication de données issues du registre AVS à la société de gestion des droits d'auteur nécessitait une base légale. Par la suite, la motion Stadler intitulée «Droit d'auteur: moins de procès, davantage d'argent pour les ayants droits» a proposé une modification de la LAVS.

Dans le cadre de la consultation des offices sur la révision des dispositions correspondantes de l'article 50a LAVS, nous avons fait part de nos réserves concernant les modalités prévues dans cette nouvelle base légale. Nous avons avant tout contesté l'extension de la finalité des données collectées par les caisses de compensation liée à l'abandon de l'obligation d'autodéclaration que la loi sur le droit d'auteur prévoit pour les utilisateurs des œuvres. Nous sommes d'avis que le passage du système de l'autodéclaration à la communication automatique des données (nom, adresse, branche et nombre de personnes employées dans l'entreprise) par les caisses de compensation aux sociétés de gestion nécessiterait une adaptation correspondante de la loi sur le droit d'auteur (LDA). Reste à relever qu'il n'est possible de calculer correctement les rémunérations pour droits d'auteur sur la base des données AVS que si le pourcentage d'emploi est connu; les caisses de compensation disposent cependant uniquement de données relatives au nombre de personnes employées.

La consultation sur la révision partielle sera close en juin 2011.

1.2.10 Révision partielle des droits réels immobiliers

Dans le cadre de la révision des droits réels immobiliers, nous avons été invités à participer à la consultation des offices sur les projets des nouvelles ordonnances d'exécution. Nos interventions ont visé à limiter au maximum les risques liés à un registre foncier tenu de manière électronique et à traiter les données avec parcimonie.

La révision partielle des droits immobiliers entraîne des conséquences au niveau des ordonnances, notamment en ce qui concerne l'introduction de la cédule hypothécaire sans titre, l'extension de l'exigence de la forme authentique pour les servitudes foncières et les droits de gage ainsi que la nouvelle réglementation sur les mentions relatives aux restrictions de propriété fondées sur le droit public. Nous avons, dans le cadre de cette révision partielle, pris position sur le projet de la nouvelle ordonnance sur le registre foncier ainsi que sur le projet d'ordonnance sur l'acte authentique électronique (OAAE). Il est prévu que les deux ordonnances entrent en vigueur le 1er janvier 2012.

La nouvelle ordonnance sur le registre foncier s'applique à une gestion informatisée du registre. Le projet prévoit déjà les bases nécessaires à l'introduction de l'échange de données d'affaires avec les bureaux du registre foncier. Conformément à l'OAAE, les documents correspondants peuvent également être remis sous forme électronique. Selon cette nouvelle ordonnance, toute personne peut demander à un bureau du registre foncier des informations concernant toutes les mentions du registre, sans devoir rendre un intérêt vraisemblable. Nous avons suggéré que, pour protéger la personnalité des propriétaires fonciers, les exceptions actuelles soient également inscrites dans la nouvelle ordonnance sur le registre foncier. Ceci concerne principalement les blocages du registre foncier dont les motifs sont étroitement liés à la personne du propriétaire foncier.

Le projet de la nouvelle ordonnance sur le registre foncier prévoit de mettre sur pied un index immobilier pour l'ensemble de la Suisse. Celui-ci doit permettre d'accéder aux données géographiques par Internet sans qu'il soit nécessaire de faire valoir un intérêt. Nous avons suggéré de prévoir une restriction tenant compte du fait que les moyens électroniques actuels (tels que la mise en relation avec des systèmes de géoinformation) permettent une mise à disposition facile et rapide dans le monde entier de données et augmentent le risque d'abus et par conséquent les possibilités d'atteintes à la personnalité. Les données peuvent facilement être copiées et utilisées de manière abusive à d'autres fins (p. ex. commerciales) par des tiers. C'est pourquoi la consultation par Internet devrait, pour des raisons de protection de la personnalité et de proportionnalité, être limitée à la désignation et à la description du bien-fonds.

Pour les autres informations qui sont également accessibles sans justification d'intérêt, toute personne peut adresser sa demande par téléphone ou par écrit ou passer personnellement au bureau du registre foncier. À notre avis, cette solution avec les données prévues devrait suffire à satisfaire l'effet publicitaire positif d'informations foncières. Par ailleurs, les responsabilités en ce qui concerne l'index immobilier suisse devraient être clairement définies dans une ordonnance du DFJP. Il s'agit en particulier d'y régler les questions concernant l'accès aux données, le contrôle et la surveillance.

Comme déjà mentionné, l'ordonnance sur le registre foncier est complétée par l'OAAE, qui contient les dispositions d'exécution du Code civil relatives à l'expédition électronique et à l'attestation authentique. Il s'agit essentiellement des points suivants:

Le projet prévoit des expéditions électroniques des actes authentiques qui reproduisent fidèlement la minute et la remplacent dans le cadre d'opérations juridiques. Ainsi que le demande l'article 55a tit. fin. CC, la minute, c'est-à-dire l'original de l'acte authentique, continue d'être dressée dans un document papier.

L'officier public certifie par une attestation authentique qu'une copie est conforme au document original ou qu'une signature provient d'une personne déterminée. L'officier public dispose d'une signature électronique qualifiée qui garantit non pas seulement qu'elle provient de sa personne, mais qui atteste également sa qualité professionnelle. La preuve de la légitimation à dresser des actes authentiques est apporté soit par la qualité professionnelle vérifiée d'officier public incluse dans le certificat, valide au moment de la signature soit par un certificat d'homologation pour chaque acte authentique obtenu séparément auprès du registre des personnes habilitées à dresser des actes authentiques, qui confirme que son détenteur est légitimé à dresser un tel acte. Il appartient aux cantons de choisir laquelle de ces deux procédures permettra d'attester cette légitimation.

L'Office fédéral de la justice confie à un organisme externe à l'administration fédérale la mise à disposition et l'exploitation d'un système pour la tenue d'un registre suisse des officiers publics. Ce registre est autofinancé par des émoluments. La Fédération Suisse des Notaires, la Fondation Notariat Suisse et des investisseurs privés ont fondé une société anonyme, dont le but est de constituer et de mettre à disposition un tel registre. À notre avis, il en particulier nécessaire de définir clairement le partage des responsabilités entre les autorités fédérales et les cantons. En outre, nous avons soulevé qu'il n'est pas nécessaire d'indiquer dans le registre le lieu de naissance ou d'origine ainsi que la nationalité de l'officier pour l'identifier.

1.2.11 Groupe de travail concernant les exigences techniques relatives à GEVER en tant que système

Il est important que les exigences de la protection des données et du principe de transparence dans l'administration soient intégrées dans le projet «GEVER Confédération» tout comme les exigences de la sécurité informatique et de la protection de l'information. Nous avons par ailleurs émis des réserves auprès de la responsable du programme quant au calendrier de migration GEVER: Seul un report du délai à fin 2013 permettrait d'intégrer les exigences dans les produits standardisés.

Dans le cadre du projet «GEVER Confédération», il a été possible d'aligner les exigences en matière de protection des données sur celles en matière de protection de l'information, tout en préservant l'indépendance fonctionnelle de chacune des classifications. Le premier niveau de protection est ainsi adapté aussi bien aux documents classifiés «internes» qu'à ceux contenant des données personnelles. Le deuxième niveau comprend quant à lui les documents classifiés «confidentiels» et ceux contenant des données personnelles sensibles ou des profils de la personnalité. Enfin, le troisième niveau est dédié aux documents classifiés «secrets» ou contenant des données personnelles dont l'abus pourrait le cas échéant impliquer un danger pour la vie de la personne concernée. Les documents de ce troisième niveau doivent pour l'instant être traités en dehors du système GEVER, tandis que les documents du deuxième niveau ne peuvent être traités dans le système que sous une forme chiffrée, afin d'en empêcher l'accès aux administrateurs et prestataires de service.

En ce qui concerne les exigences devant permettre de garantir la transparence administrative conformément à la loi sur la transparence (LTrans), l'accessibilité de chaque document GEVER doit pouvoir être définie tout d'abord par son auteur à titre indicatif et ensuite par l'autorité qui traite une demande concrète d'accès à ce document. L'accès peut ainsi être «différé», «accordé», «partiellement accordé», «refusé»; le statut d'accès peut également avoir la valeur «inapplicable», lorsque l'autorité estime que la LTrans n'est pas applicable. En outre, le statut d'accès peut être modifié par l'autorité concernée suite à une procédure de médiation initiée par le demandeur, le cas échéant assortie d'une recommandation du préposé, ou suite à une décision du Tribunal administratif fédéral ou en dernier lieu du Tribunal fédéral. En complément du statut d'accès des documents, le système GEVER doit aussi – conformément à la loi – permettre à chaque autorité de fournir des statistiques annuelles concernant le nombre de demandes d'accès reçues, la répartition des statuts d'accès définis ainsi que le montant total des émoluments exigés.

S'agissant du calendrier de la migration GEVER, nous avons émis des réserves auprès de la responsable du programme «GEVER Confédération». Avec une approbation du catalogue d'exigences techniques planifiée par la Conférence des secrétaires généraux pour l'été 2011, il est en effet probable qu'aucun des deux produits actuellement standardisés ne sera à même d'intégrer les fonctionnalités attendues jusqu'à fin 2011. En conséquence, tous les documents du niveau de protection 2 (confidentiels ou sensibles) ne pourront être protégés de manière adéquate dans GEVER tant et aussi longtemps que les produits standardisés ne satisferont pas aux exigences techniques formulées. Partant, nous sommes d'avis que la date limite d'introduction des systèmes GEVER dans les offices initialement prévue à fin 2011 par la décision du Conseil fédéral du 23 janvier 2008 devrait être reportée à fin 2013. Un tel report coïnciderait avec les mesures complémentaires portant sur la mise en œuvre des exigences en matière de protection de l'information et de protection des données décidées le 16 décembre 2009 et confirmées le 4 juin 2010 par le Conseil fédéral.

1.3 Internet et télécommunication

1.3.1 Rester anonyme sur le Web?

Est-il possible aujourd'hui de rester anonyme lorsque l'on navigue sur le Web? Les cookies par exemple sont de plus en plus performants pour permettre une personnalisation des navigateurs web. Mais, bien au-delà de cette technologie, on constate que le navigateur utilisé laisse lui-même une empreinte qui nous identifie de manière unique. Nous avons pu confirmer ce constat en étudiant puis en testant l'algorithme Panopticlick.

Depuis les débuts du Web, les cookies permettent d'améliorer notre confort de navigation. Ces petits fichiers sont déposés sur nos ordinateurs lors de la visite d'un site web, sauvegardant les préférences de l'utilisateur (telles que la langue dans lequel un site doit s'afficher par exemple), et permettant ainsi au site de «reconnaître» l'utilisateur lors d'une visite future.

Au-delà de la technologie des cookies, des chercheurs ont fait le constat suivant: chaque navigateur web a une empreinte et chaque empreinte est unique, ou presque. Ainsi, il n'y a plus besoin de cookies pour déterminer quel ordinateur s'est connecté à un site web, il suffit d'observer l'empreinte du navigateur utilisé.

Nous avons étudié et testé l'algorithme Panopticlick (panopticon étant un modèle de prison qui permet aux gardiens d'observer les prisonniers sans se faire remarquer) proposé par Electronic Frontiers Foundation. Cet algorithme considère un certain nombre de paramètres en entrée et rend une mesure d'entropie qui permet de déterminer l'unicité du navigateur testé. Les paramètres sont, par exemple, le user agent qui donne des informations sur le type et la version du navigateur mais aussi du système d'exploitation utilisé, la liste des plug-ins installés – un plug-in étant un petit logiciel qui complète le navigateur en lui faisant bénéficier de nouvelles fonctionnalités, telles que la lecture de vidéos, les polices de caractère installées, des informations sur l'écran utilisé, etc. En fait, toutes les informations auxquelles il est possible d'accéder à travers le navigateur sont collectées. Ces informations mises bout à bout sont considérées comme l'identifiant (empreinte) du navigateur. Ainsi, c'est l'éventuelle unicité de cet identifiant qui détermine l'unicité du navigateur.

Dans la première phase de déploiement de l'algorithme, environ 400'000 empreintes ont été récoltées et anonymisées. Chaque nouvelle empreinte est testée par rapport à cet ensemble. Il est ainsi possible de déterminer si cette empreinte est semblable à

l'une de celles déjà connues. Si c'est le cas, on détermine combien d'empreintes doivent être inclues dans un sous-ensemble pour être certain d'y trouver une empreinte identique.

Nous avons testé cet algorithme avec les dernières versions des navigateurs les plus connus (Internet Explorer, Firefox, Chrome, Safari, Opera) sous diverses conditions: directement après l'installation du navigateur, après un temps de navigation, en mode anonyme et après l'ajout de certaines extensions.

La conclusion que nous faisons est la suivante: il faut effectivement admettre que l'empreinte de chaque navigateur est unique, ou facilement identifiable. Il existe toutefois des possibilités de réduire quelque peu les dangers d'une identification certaine. Ainsi, le mode de navigation anonyme qui est aujourd'hui proposé par l'ensemble des navigateurs (du moins dans leur dernière version) est un bon outil à exploiter. Couplé à certaines extensions, comme NoScript, proposées en particulier par le navigateur Firefox, il est le meilleur moyen de préserver son anonymat lors de la navigation sur le Web.

1.3.2 Nouvelle évolution des cookies

Dans le cadre de nos activités de veille technologique, nous avons étudié les développements liés à l'utilisation des cookies. Les cookies sont un mécanisme bien connu des navigateurs web qui permet de conserver une trace de l'utilisateur. Ils sont en quelque sorte la mémoire des navigateurs. Avec l'évolution des technologies, ces cookies, à l'origine de simples petits fichiers, sont devenus de plus en plus puissants et sont ainsi une véritable menace pour la sphère privée.

Un cookie est un petit fichier envoyé par un site web lors d'une première visite à un navigateur qui est renvoyé par le navigateur au site à chaque nouvelle visite. Il permet au site web de reconnaître le navigateur et par conséquent, l'ordinateur et l'utilisateur. Ainsi, certaines préférences de l'utilisateur peuvent être mémorisées et réactivées par le site à chaque visite.

Une première évolution des cookies a été l'apparition des cookies tierce partie. Ceux-ci ne sont pas déposés sur la machine par le site visité mais par un site tiers dont des objets – des encarts de publicité par exemple – apparaissent sur la page visitée. Il s'agit d'une atteinte plus conséquente à la vie privée puisque l'utilisateur ne peut pas s'attendre à recevoir ces cookies. Si les publicités d'un même site apparaissent sur plusieurs autres sites, l'utilisateur peut être suivi dans sa navigation par la trace laissée par les cookies tierce partie.

Les Flash cookies (local shared objects) sont des cookies beaucoup plus importants en terme de taille de fichiers. L'information qu'ils peuvent contenir est donc également beaucoup plus conséquente. De plus, ces cookies ont la propriété d'être visibles par différents navigateurs et non pas seulement par le navigateur qui était utilisé au moment du dépôt du cookie sur l'ordinateur.

Finalement, la dernière évolution des cookies que nous avons constatée est l'apparition de evercookies. Ces cookies ont la faculté de se répliquer et d'introduire des copies dans différents espaces du PC. Pour supprimer un tel cookie, il ne faut pas seulement effacer le cookie mais également la totalité de ses copies – il peut y en avoir jusqu'à 13. Il suffit qu'une seule copie soit oubliée pour que le cookie se réplique automatiquement. Il est impossible pour l'utilisateur de supprimer les cookies de manière usuelle pour retrouver un certain anonymat vis-à-vis des sites qu'il visite.

Différents tests nous ont permis de constater que ces evercookies sont extrêmement difficiles à supprimer. Il faut combiner différentes techniques de suppression et il subsiste toujours des copies qui ne peuvent être détruites de manière simple. Pour répondre à cette nouvelle technologie, différents projets sont en cours de développement mais ne pouvaient être considérés comme fiables lors de nos tests.

L'évolution des cookies montre qu'il est de plus en plus difficile de rester anonyme lorsque l'on navigue sur le Web. Ces informations introduites dans les ordinateurs et difficilement supprimables renseignent les sites web sur les habitudes de navigation de chaque utilisateur et, par conséquent, sur ses goûts, ses centres d'intérêts, etc.

1.3.3 Prises de vue des voies publiques sur Internet

Google ne voulant pas suivre nos recommandations visant une mise en œuvre de son service Street View respectueuse de la protection des données, nous avons soumis le cas à l'appréciation du Tribunal administratif fédéral. Ce dernier a approuvé nos exigences sur tous les points essentiels. Par ailleurs, nous avons examiné les procédés d'autres fournisseurs de prises de vue des voies publiques sur Internet. Ils se différencient de Google Street View à divers égards.

Comme nous l'avons déjà indiqué dans notre 17e rapport d'activités 2009/2010, ch. 1.3.2, Google avait refusé de se conformer à nos recommandations visant à respecter de manière appropriée les principes de la protection des données. Nous avons donc engagé une action devant le Tribunal administratif fédéral (TAF). Celui-ci a rendu son jugement le 30 mars 2011. Il y confirme que la légalité de Google Street View, vues sous l'angle du droit de la protection des données, sont soumises au droit suisse et que le

PFPDT est effectivement habilité à adresser une recommandation à Google Street View. Google avait contesté ces deux points.

Selon le TAF, Google devra désormais veiller à ce que tous les visages et plaques de contrôle soient rendus méconnaissables avant leur publication. Les images devront être contrôlées manuellement tant que l'anonymisation fondée sur un programme informatique ne sera pas entièrement fiable. En outre, sur les images prises à proximité des endroits considérés comme sensibles, par exemple les prisons, les hôpitaux ou les centres d'accueil pour les femmes, l'anonymat doit être garanti par la suppression d'autres caractéristiques personnelles comme la couleur de la peau, l'habillement, les moyens auxiliaires utilisés par les handicapés, etc. Google n'est plus autorisé à photographier les domaines privés tels que les jardins ou cours intérieures fermés, inaccessibles aux regards d'un passant ordinaire, et doit retirer de son site Street View les images de ce type déjà publiées s'il n'a pas obtenu le consentement des personnes concernées. Une semaine avant, Google doit informer la population sur Internet et dans les médias locaux de son passage et de la publication de nouvelles images.

Le jugement du Tribunal administratif fédéral n'était pas encore entré en force au moment de la clôture de rédaction de notre rapport d'activités. Mais grâce à l'exposé convaincant de ses motifs, il contribue en tout état de cause à clarifier de manière déterminante la question de la délimitation entre les intérêts économiques des fournisseurs de nouvelles applications en ligne et les intérêts des personnes concernées quant à la protection de leurs droits de la personnalité. Ce jugement du TAF (A-7040/2009) peut être consulté sur notre site ou sur celui du Tribunal administratif fédéral.

Nous avons procédé à des examens des faits concernant quatre autres services proposant des «promenades» virtuelles sur Internet et avons constaté que ces fournisseurs prenaient tous des mesures pour protéger les droits de la personnalité. Toutefois, chaque service présente des caractéristiques spécifiques, notamment en ce qui concerne les modalités concrètes de la prise de vue et de la publication. Les moyens techniques utilisés, les procédures et les méthodes se différencient considérablement de celles de Google Street View. C'est de manière tout aussi différenciée que la pondération des intérêts doit avoir lieu et que les mesures appropriées relatives à la protection des données doivent être développées.

Sur les autres sites que nous avons examinés, les prises de vue – contrairement à celles de Google Street View – ne couvrent pas l'ensemble du territoire et ne sont pas effectuées automatiquement à partir du toit d'une automobile en marche, mais à partir d'emplacements déterminés situés dans le domaine public, à l'aide d'une caméra numérique montée sur un pied à hauteur d'yeux et munie d'un objectif grand angle. À chaque emplacement, des photos sont prises dans toutes les directions, pendant une

certaine durée. Les passants éventuels ont donc la possibilité de reconnaître qu'ils sont photographiés et peuvent soit détourner la tête, soit quitter le secteur photographié. En outre, le photographe, par le choix du moment de la prise de vue, peut éviter que les personnes qui ne le souhaitent manifestement pas figurent sur la photo. Etant donné que le photographe se déplace à pied et ne se trouve pas dans une voiture en marche, il peut aussi être abordé directement pas les personnes présentes. Celles-ci peuvent donc s'informer du but des prises de vue et de leur utilisation postérieure, ou encore s'opposer à leur publication.

En outre, les photos font ultérieurement l'objet d'un traitement manuel individuel (et non pas comme chez Google Street View à l'aide d'un logiciel entièrement automatisé, mais susceptible de commettre des erreurs). À cette occasion, les personnes photographiées sont rendues encore plus méconnaissables par floutage ou par superposition de plusieurs images prises à brefs intervalles.

Les exemples que nous avons examinés ne montrent pas seulement comment il est possible de mieux respecter les exigences de la protection des données en optant pour une autre méthode technique, mais aussi que des solutions créatives ont été trouvées permettant de donner un «effet de vie» aux images publiées tout en respectant les droits de la personnalité des passants qui y sont représentés.

1.3.4 Recensement de réseaux sans fil

Au printemps 2010, on a appris que Google avait, lors de ses courses effectuées pour Street View en Suisse, également enregistré des données provenant de réseaux Wi-Fi. Nos recherches ont révélé que l'enregistrement de ces données n'était pas conforme aux exigences de la protection sur les données.

En avril 2010, nous avons procédé à des examens relatifs au recensement de réseaux sans fil par Google et avons prié la société de prendre position. Début mai 2010, Google nous a communiqué par écrit que la société enregistrait et traitait effectivement des données relatives aux réseaux Wi-Fi présents en Suisse, mais qu'elle ne collectait pas de contenus des communications (données de charge utile). Elle précisait que le but de cette saisie de données était de pouvoir mettre en service une fonction de localisation qui soit indépendante d'un signal GPS en se basant sur les emplacements des antennes et des routeurs Wi-Fi. Puis, à mi-mai 2010 déjà, Google nous a informés que la société avait, lors de ces courses de prises de vue pour Street View, malgré tout enregistré sans s'en rendre compte des contenus de communications en provenance de réseaux Wi-Fi non protégés. Par la suite, Google a cessé les courses de prises de vue jusqu'à ce que les équipements Wi-Fi installés sur les véhicules soient démontés.

Immédiatement après la divulgation de l'enregistrement de ces données, Google a extrait ces données de son réseau d'entreprise pour les chiffrer et les bloquer pour tout usage ultérieur. Lors de l'analyse de ces données, nous avons découvert des extraits de communication sans fil qui ont eu lieu juste au moment où le véhicule Street View traversait la zone d'émission du point d'accès Wi-Fi. Il s'agit entre autres de courriels complets, d'appels de sites web, de noms d'utilisateurs, de mots de passe, numéros de téléphone, adresses de courriel et adresses d'entreprises. Nos découvertes coïncident ainsi avec celles faites par d'autres autorités de protection des données.

Les équipements Wi-Fi ayant été enlevés des véhicules de prise de vue, Google n'enregistrera plus de données de charge utile lors de ses futures courses. Nous avons recommandé à la société de détruire la totalité des données de charge utile qu'elle a collectées de manière illicite et de prendre des mesures sur le plan technique et organisationnel pour éviter que des incidents comparables ne puissent se reproduire. Il s'agira en particulier de tenir compte des exigences de la protection de la sphère privée dès la phase de développement («Privacy by Design») et de mener des audits avant de proposer de nouveaux services et produits.

Nos recherches ont en outre montré qu'un grand nombre de réseaux locaux sans fil étaient encore toujours exploités sans cryptage. Nous avons notamment été surpris par le fait que non seulement des informations privées, mais aussi des informations de nature commerciale (telles qu'un courriel concernant un projet de création d'un entrepôt de données dans une banque), étaient transmises par le biais de réseaux locaux sans fil sans avoir été préalablement chiffrées. Nous recommandons vivement de n'exploiter les réseaux locaux sans fil que sous forme chiffrée (WPA2-AES), ceci afin d'éviter d'une part que des tiers n'aient accès aux données qui y circulent et, d'autre part, que des clandestins ne se branchent sur le réseau et restreignent ainsi la largeur de la bande ou encore s'en servent pour mener des actions illégales. Nous conseillons par ailleurs de chiffrer les informations confidentielles, même lorsqu'elles sont transmises par le biais de connexions sécurisées ou chiffrées (SSL, VPN).

1.3.5 Échanges de contenus sur Internet: Arrêt du Tribunal fédéral

Le Tribunal fédéral a ordonné à la société Logistep AG de suspendre tout traitement de données dans le domaine des droits d'auteur et lui a interdit de transmettre les données déjà collectées aux détenteurs concernés de ces droits. Il entend ainsi marquer clairement son opposition envers la tendance, déjà constatée dans d'autres domaines, de certains particuliers qui s'attribuent des tâches revenant clairement à l'État de droit.

Sur mandat de détenteurs de droits d'auteurs, la société Logistep AG collectait dans des réseaux pair-à-pair (P2P) des adresses IP d'utilisateurs qui offraient apparemment de manière illégale des contenus protégés par les droits d'auteur (fichiers musique ou vidéo). Sur la base de ces adresses IP, les détenteurs de ces droits engageaient des procédures pénales afin d'établir l'identité des personnes concernées et de leur réclamer des dommages et intérêts. À notre avis, ce traitement n'était pas reconnaissable pour les personnes concernées et allait à l'encontre du principe de finalité sans motif justificatif. Début 2008, nous avons recommandé à Logistep d'interrompre ses recherches dans les réseaux pair-à-pair tant que le législateur n'aurait pas créé de base légale pour cela (cf. notre 15e rapport d'activités 2007/2008, ch. 1.3.1).

Logistep a rejeté notre recommandation. Nous avons donc porté le cas devant le Tribunal administratif fédéral (TAF). Estimant que les intérêts des détenteurs des droits d'auteur primaient sur ceux des utilisateurs P2P, le TAF a rejeté notre action par jugement du 27 mai 2009 (cf. notre 16e rapport d'activités 2008/2009, ch. 1.3.1).

Nous avons soumis le jugement du TAF au verdict du Tribunal fédéral qui a cassé le jugement de première instance et s'est ainsi rangé à notre avis: il a ordonné à la société Logistep d'interrompre tout traitement de données dans le domaine des droits d'auteur et lui a interdit de transmettre les données déjà collectées aux détenteurs des droits d'auteur concernés (arrêt 1C_285/2009 du 8 septembre 2010).

Le jugement rendu par la plus haute juridiction suisse a une portée qui dépasse le cas d'espèce. Nous présentons ci-dessous ses principaux considérants:

- En cas de communication de données, il suffit que le destinataire soit en mesure d'identifier les personnes concernées pour que les données puissent être qualifiées de données personnelles. Dans ce cas, la loi sur la protection des données est applicable à l'ensemble du traitement des données.

- Il n'est pas possible de constater de manière abstraite si des adresses IP (notamment les adresses IP dynamiques) sont des données personnelles ou pas; chaque cas doit être considéré comme un cas d'espèce. Les adresses IP sont dans tous les cas des données personnelles lorsqu'il semble fort probable que l'on pourrait déterminer la personne en question. Tel était ici le cas car toute la structure de fonctionnement de Logistep reposait sur l'identification des personnes concernées.

- En traitant ainsi des données, la société Logistep a violé le principe de finalité et l'exigence de reconnaissabilité. Il s'agissait d'examiner si elle avait pour cela un motif justificatif. De l'avis du TF, une interprétation strictement systématique selon laquelle on ne peut faire valoir un motif justificatif que dans les cas présentés aux lettres b et c, et non à la lettre a de l'art. 12, al. 2, LPD est inopportun car, même si dans la version actuelle de la lettre a les motifs justificatifs ne sont plus mentionnés, ils n'en sont pas non plus expressément exclus. La disposition doit donc être interprétée en ce sens qu'une justification du traitement de données personnelles en violation des principes figurant aux art. 4, art. 5, al. 1, et art. 7, al. 1, LPD ne peut certes être exclue d'une manière générale, mais que les motifs justificatifs ne peuvent être admis concrètement qu'avec une grande réserve.

- La recommandation du PFPDT a pour objectif de défendre un grand nombre de personnes et est donc en définitive dans l'intérêt public. Il faut tenir compte de cet aspect de la recommandation du PFPDT dans la pondération des intérêts en vertu de l'art. 13, al. 1, LPD d'autant plus qu'une recommandation (le cas échéant confirmée par le tribunal) produit un effet indirect pour toutes les personnes qui procèdent selon une méthode similaire.

- En recherchant, dans des réseaux P2P, des œuvres protégées par les droits d'auteur à l'aide d'un logiciel développé à cet effet et en stockant les données, la société Logistep poursuivait des buts économiques. D'une manière générale, c'est-à-dire au-delà du cas qui nous occupe ici, ce genre de méthode mène, du fait de l'absence de réglementation légale, à une insécurité en ce qui concerne le genre et le volume des données collectées sur Internet et leur traitement. En particulier, le stockage et l'utilisation possible des données en dehors d'une procédure judiciaire ordinaire ne sont pas clairement déterminés. Même l'intérêt d'une lutte efficace contre les violations des droits d'auteur ne permet pas de contrebalancer la portée des atteintes à la personnalité et des incertitudes qui accompagnent le procédé contesté concernant le traitement de données sur Internet.

- Pour le Tribunal fédéral, il ne s'agissait pas explicitement de donner d'une manière générale à la protection des données la primauté face à la protection du droit d'auteur. Mais il estime qu'il appartient au législateur, et non au juge, de prendre les mesures nécessaires afin de garantir une protection des droits d'auteur conforme aux technologies les plus récentes.
- Le Tribunal fédéral a expressément laissé en suspens la question de l'utilisation par les autorités de poursuite pénale des données recueillies par Logistep.

1.3.6 Marketing en ligne: Nouvelle directive «Vie privée et communications électroniques» de l'UE

Le Parlement européen a décidé à la fin de l'année 2009 de procéder à une révision de la directive 2002/58/CE vie privée et communications électroniques. Le but est d'améliorer la transparence et la sécurité pour les consommateurs. La mise en oeuvre pratique de la nouvelle directive dans les États membres devrait se concrétiser à partir de 2011, ce qui entraînera également des conséquences pour la Suisse.

La directive «Vie privée et communications électroniques» (e-privacy) a été élaborée pour répondre aux exigences des nouvelles technologies numériques. Cette directive complète la directive de l'Union européenne sur la protection des données et couvre tous les thèmes de la sphère privée dans le secteur de la communication électronique. La directive règle la protection des données personnelles et de la sphère privée dans les réseaux de communication électroniques.

La nouvelle directive 2009/136/CE oblige pour la première fois les fournisseurs de services à informer de manière active leurs utilisateurs sur les incidents survenus au niveau des données ainsi que sur les risques spécifiques tels que virus ou attaques de logiciels malveillants.

Une autre nouveauté: les cookies ou logiciels espions ne pourront dorénavant plus être installés sur le PC de l'utilisateur Internet sans son consentement. Les cookies peuvent mémoriser données de connexion, mots de passe ou préférences, ce qui est très pratique pour l'utilisateur. Ils peuvent cependant également être utilisés pour suivre les activités de l'utilisateur sur la Toile. En répartissant ces cookies sur plusieurs sites web, certaines entreprises de publicité sont ainsi en mesure de créer des profils d'utilisation. Ce procédé est connu sous le nom de «Online Tracking».

L'ancienne directive demandait aux exploitants de sites web de donner aux utilisateurs une option de retrait (opt-out). Ils pouvaient le faire de manière appropriée en installant les paramètres du navigateur web. La nouvelle directive de l'Union européenne prévoit

désormais que les utilisateurs doivent donner leur consentement explicite pour l'enregistrement d'informations ou pour l'accès à de telles informations (option d'adhésion ou «Opt-in»). Cela signifie que les utilisateurs doivent recevoir au préalable des informations claires et détaillées sur les finalités de l'enregistrement ou de l'accès.

Les États membres de l'UE doivent mettre en oeuvre cette directive dans leurs législations nationales d'ici au 25 mai 2011. Comment ceci va se concrétiser dans les divers pays est actuellement discuté entre les fournisseurs de prestations Internet, les entreprises de publicité, les autorités législatives et celles de protection des données.

La Suisse n'étant pas membre de l'UE, le droit communautaire n'est applicable que si elle le décide explicitement. Quoi qu'il en soit, ces réglementations auront également des répercussions sur les fournisseurs et utilisateurs domiciliés en Suisse. C'est pourquoi nous suivons de très près ces discussions. Nous avons d'autre part noué des contacts avec diverses associations professionnelles nationales et internationales et sommes en constante discussion afin d'évaluer les conséquences pour les entreprises suisses et trouver des solutions.

Sur le fond, nous approuvons les modifications envisagées en faveur d'une pratique plus respectueuse de la protection des données dans le domaine du marketing en ligne, en utilisant des cookies et des instruments similaires. Celle-ci doit cependant être à la fois conviviale et facile à utiliser.

1.3.7 Réseaux sociaux et protection des données

Les services de réseaux sociaux sur Internet ont toujours le vent en poupe. Vu les implications internationales, la situation juridique est souvent compliquée. Les utilisateurs d'Internet seraient bien avisés de prendre leurs responsabilités et de ne publier leurs données personnelles qu'avec circonspection.

Nous recevons régulièrement des questions au sujet des réseaux sociaux sur Internet. Mais bon nombre de points demeurent encore obscurs, en particulier en ce qui concerne le champ d'application territorial des législations nationales sur la protection des données lorsque les fournisseurs de services Internet ont leur siège à l'étranger. Les actions en justice contre ces fournisseurs sont longues et difficiles. Nous observons de près le développement de ces réseaux sociaux et examinons, en collaboration avec des offices étrangers de protection des données, les possibilités d'action afin de faire aussi respecter dans un média de portée mondiale comme Internet le droit fondamental de l'individu à la libre disposition des informations le concernant.

La fonction «Recherche d'amis» sur Facebook a suscité de nombreuses questions de particuliers. Facebook part du principe qu'une personne est en relation avec d'autres lorsque celles-ci transmettent son adresse électronique à Facebook, par exemple en téléchargeant leur carnet d'adresses électroniques sur la plate forme par le biais de la fonction «Recherche d'amis». S'appuyant sur cette supposition, Facebook envoie des courriels publicitaires personnalisés avec l'indication d'«amis» potentiels afin de gagner de nouveaux utilisateurs.

Nous recommandons aux personnes concernées de signaler à leurs amis qu'elles ne souhaitent pas que leurs données personnelles soient transmises à Facebook. Facebook met en outre à leur disposition une fonction (pas tout à fait simple à trouver) permettant de stopper tout futur courrier électronique: on trouvera à l'adresse www.facebook.com/help/contact.php?show_form=database_removal un formulaire permettant d'indiquer que l'on veut être retiré de la banque de données et que l'on ne veut plus recevoir de courriers électroniques de la part de Facebook.

Nous avons déjà signalé les risques et les dangers des réseaux sociaux dans notre 16e rapport d'activités 2008/2009, ch. 1.3.6, et exprimé des recommandations concrètes quant à une utilisation responsable des réseaux sociaux. Un dossier thématique est également disponible sur notre site web (Thèmes – Protection des données – Internet – Réseaux sociaux).

1.3.8 Traitement de données de clients dans les entreprises de télécommunication

L'industrie des télécommunications se développe dans un marché innovant et évoluant très rapidement. Du point de vue de la protection des données, la gestion correcte et la mise à jour des adresses des clients d'une entreprise doivent suivre le rythme de l'évolution technologique et pouvoir être garanties en tout temps.

En 2007 et 2008, nous avons à plusieurs reprises été contactés par des clients d'une entreprise de télécommunication dont les demandes de modification d'adresse (pour cause de déménagement ou de changement de nom) n'avaient pas été correctement traitées. C'est pourquoi nous avons, l'an passé, procédé à un examen des faits auprès de cette entreprise. Ce dernier a surtout porté sur la correction des données client et leur gestion subséquente. Une attention particulière a été portée à la manière dont sont traités les avis de déménagement ainsi que sur les mesures techniques et organisationnelles pour leur saisie.

L'entreprise de télécommunication a essentiellement confirmé les problèmes qui nous ont été rapportés jusqu'en automne 2009. Elle avait d'ailleurs déjà pris des mesures au

niveau de l'organisation et de la structure du service «Office Operations». Elle a également fait remarquer que le délai de traitement pour un changement d'adresse était d'un mois environ à compter de la date de réception. Selon elle, de nombreux clients ne sont pas conscients du fait qu'un changement d'adresse ne peut pas se faire du jour au lendemain. Ceci vaut notamment pour les cas où la facturation et le traitement de la modification de l'adresse ont lieu en parallèle, de sorte que, à cause du délai d'attente, la facture peut encore être envoyée à l'ancienne adresse. Il est en particulier très probable que de nombreux clients qui ont modifié eux-mêmes leurs données d'adresse sur le site web s'attendent à ce que ce changement prenne effet immédiatement. L'entreprise relève que depuis un certain temps elle indique ce délai d'un mois à ses clients, tant sur son site web que par téléphone, et qu'elle a, de manière générale, amélioré la qualité de son service client.

Au niveau marketing et publicité, l'entreprise nous a confirmé qu'elle ne vendait ni ne louait les adresses de ses clients à des tiers. Elle a également précisé qu'elle n'enregistrait aucune donnée sur l'usage de ses prestations par les clients, mais que les données absolument nécessaires pour la facturation, et qu'elle n'établissait pas d'analyse ou de profils. Ceci vaut également pour le domaine de la télévision numérique où aucune analyse du comportement des consommateurs ne serait effectuée (même pas de manière anonymisée).

Dans l'ensemble, nous pouvons conclure sur la base des informations et des documents reçus qu'il n'y avait plus de problèmes au niveau de l'administration des adresses client auprès de cette entreprise de télécommunication au moment où notre examen des faits a eu lieu. L'entreprise a réagi aux difficultés survenues par le passé et a corrigé ses processus. D'ailleurs, le nombre des plaintes reçues depuis novembre 2009 a nettement diminué. Nous avons constaté que l'entreprise est consciente du devoir de diligence qu'elle a envers les adresses de ses clients. Ce soin se fait également sentir au niveau de l'infrastructure informatique et de sa gestion. Nous avons finalement proposé à l'entreprise de régler directement avec nous toute question relative à la protection des données.

1.3.9 Traitement de données personnelles dans le cadre de systèmes GEVER supradépartementaux

La base légale pour le traitement de données personnelles dans un système GEVER au niveau des organes de la Confédération se trouve à l'article 57h de la loi sur l'organisation du gouvernement et de l'administration (LOGA). Cette disposition ne suffit cependant pas comme base légale pour un système GEVER supradépartemental dans le cadre d'une procédure automatisée.

Dans l'administration fédérale, le terme GEVER est utilisé pour tout système de gestion électronique des affaires. L'objectif de ce système est en principe de permettre, moyennant une gestion systématique, une tenue des documents efficace et conforme à la loi ainsi qu'une mise à disposition rapide des informations. Ce système constitue également la condition de base pour des processus automatisés de bout en bout dans le domaine de la cyberadministration. Il est donc prévu, dans le cadre du programme GEVER de la Confédération, de transposer les affaires du Conseil fédéral et du Parlement sous forme de processus supradépartementaux gérés de manière électronique de bout en bout (donc sans rupture de média) d'ici la fin de l'année 2011.

Pour pouvoir traiter des données personnelles sensibles et des profils de la personnalité, les organes fédéraux doivent pouvoir s'appuyer sur une base légale au sens formel. Cette base légale existe à l'article 57h LOGA, qui permet à tout organe fédéral d'exploiter un système d'information et de documentation. Ce dernier peut contenir des données sensibles et des profils de la personnalité, dans la mesure où ceux-ci ressortent de la correspondance ou découlent de la nature de l'affaire. Cette règle ne s'applique cependant qu'à la gestion des affaires au sein d'un organe fédéral, soit d'un office ou d'un département. Le législateur ne voulait pas que l'accès automatique à de tels systèmes soit accordé à plusieurs organes fédéraux. C'est pourquoi il a précisé dans le deuxième alinéa de cet article que «seuls les collaborateurs de l'organe concerné ont accès à des données personnelles, et uniquement dans la mesure où ces données sont nécessaires à l'accomplissement de leurs tâches.»

Ceci soulève la question de la base légale nécessaire pour une gestion des affaires supradépartementale ou supra-office. Nous en avons débattu à plusieurs reprises avec les représentants de GEVER Confédération. À notre avis, l'article 57h LOGA n'est pas suffisant pour un système GEVER basé sur des processus supradépartementaux automatisés, si celui-ci inclut des traitements de données personnelles sensibles ou de profils de la personnalité. Il faudrait donc le cas échéant adapter cette disposition et étendre son champ d'application.

1.3.10 Accomplissement électronique des formalités de douane

Le projet eCustoms de l'Union européenne vise à remplacer l'ensemble des procédures douanières sur support papier par des procédures électroniques, afin de créer un environnement douanier plus efficace et plus moderne. Un groupe de travail que nous avons accompagné a élaboré une étude de faisabilité concernant une éventuelle participation de la Suisse à ce projet.

L'objectif du projet eCustoms est de traiter toutes les opérations douanières (import, export, transit) de manière simple et efficace par l'intermédiaire d'un seul portail Internet. L'échange de données entre les fournisseurs, les bureaux de douane à l'intérieur du pays et à l'étranger et les clients devrait se faire de manière électronique de bout en bout. Sur le plan national, cela implique que nous devons appliquer nos principes de cyberadministration aux procédures douanières. Sur le plan international, cela signifie en particulier que les systèmes électroniques de dédouanement de la Suisse et de l'UE seraient reliés entre eux.

Un groupe d'experts interdépartemental, composé de représentants du DFE, du DFF, du DFAE et du DFJP, a élaboré une étude de faisabilité concernant une participation de la Suisse au projet eCustoms. Cette dernière servira de base de décision au Conseil fédéral en vue d'éventuelles négociations avec l'UE.

Nous avons, en coordination avec l'Office fédéral de la justice, accompagné le projet en ce qui concerne la protection des données. Nous avons entre autres constaté que la loi sur les douanes ainsi que l'ordonnance sur le traitement des données dans l'administration fédérale des douanes nécessitent une adaptation. Il était cependant trop tôt au moment de l'élaboration de l'étude de faisabilité pour évaluer quelles dispositions doivent concrètement être modifiées, étant donné que de nombreuses questions concernant la réalisation du projet eCustoms n'ont pas encore trouvé réponse. Ce n'est qu'au moment de la concrétisation du projet que nous serons en mesure d'évaluer quelles adaptations sont effectivement nécessaires et quels sont les aspects auxquels il y a lieu d'attacher une importance spéciale du point de vue de la protection des données.

1.4 Justice/Police/Sécurité

1.4.1 Application de l'accord de Schengen: contrôle auprès du Consulat général à Istanbul

Nous avons, dans le cadre de la coopération Schengen, effectué un contrôle auprès du Consulat général d'Istanbul. Notre examen a entre autres porté sur la gestion des rendez-vous par une entreprise turque ainsi que sur les fichiers de journalisation.

Pour la troisième fois, nous avons effectué un contrôle auprès d'une représentation de la Suisse à l'étranger dans le cadre de la coopération Schengen. De tels examens ont principalement pour but de vérifier la délivrance de visas Schengen ainsi que le traitement correspondant de données dans le système d'information Schengen (SIS). Cette année, nous avons effectué notre contrôle auprès Consulat général d'Istanbul, où la gestion des rendez-vous pour les requérants de visas a été confiée à une entreprise privée turque. Une telle externalisation est autorisée par le droit Schengen, mais elle est soumise à des exigences sévères. Nos contrôles ont porté sur l'ensemble du traitement des données lié à la délivrance des visas Schengen ainsi que sur l'externalisation de la gestion des rendez-vous. Dans ce cadre, nous avons également examiné les accès du consulat au SIS et au système d'information SYMIC de l'Office fédéral des migrations (ODM) de même que les fichiers de journalisation correspondants. Pour ce faire, nous avons noté sur place un certain nombre de consultations de données effectuées dans les systèmes SIS et SYMIC et vérifié ensuite à Berne – auprès de fedpol pour le système SIS et auprès de l'ODM pour le système SYMIC – si ces accès avaient bel et bien été journalisés.

Nous avons pu constater que les traitements de données que nous avions examinés avaient été effectués en conformité avec les prescriptions de la protection des données. Nos contrôles ont abouti uniquement à deux propositions d'amélioration qui ont toutes deux été acceptées. La première proposition s'adressait au Consulat général, respectivement au Département fédéral des affaires étrangères et précisait que la formation encore inachevée du personnel concerné en matière de protection des données devait être terminée d'ici la fin de l'année 2011. La deuxième proposition s'adressait à l'ODM. En vérifiant la liste des utilisateurs du système SYMIC, nous avons constaté la présence d'un compte qui n'était pas rattaché à une personne précise, mais libellé «Épuration des données». Nous avons proposé à l'ODM de modifier le nom de ce compte utilisé à des fins d'assistance en le mettant au nom du collaborateur chargé de cette tâche. Pour le cas où plusieurs personnes assumeraient des tâches d'assistance, nous avons suggéré d'ouvrir des comptes personnalisés supplémentaires.

1.4.2 Mise en œuvre Schengen: contrôle auprès du Corps des gardes-frontière

Le contrôle que nous avons effectué auprès du Corps des gardes-frontière a montré que les collaboratrices et collaborateurs concernés ont consulté le Système d'information Schengen de manière conforme aux exigences légales en la matière. Des éclaircissements sont cependant nécessaires dans le domaine de la formation des utilisateurs.

Dans le cadre de nos compétences de surveillance des traitements de données personnelles effectués par des organes fédéraux utilisateurs de la partie nationale du Système d'information Schengen (N-SIS), nous avons procédé au contrôle des accès au N-SIS des collaboratrices et des collaborateurs d'une région du Corps des gardes-frontière. Nous avons effectué notre analyse à partir des logfiles du N-SIS. Nous avons vérifié les accès de la moitié des collaborateurs en service (environ 50 personnes) dans la période retenue (un samedi et un dimanche). Au total, ces collaborateurs ont recherché une vingtaine de personnes dans le N-SIS dans la période en question.

Une personne en service a effectué des recherches dans le N-SIS avec son propre nom de famille. Nous avons effectué une nouvelle analyse des logfiles du N-SIS concernant cette personne portant sur une période de sept mois et avons constaté que celle-ci avait procédé quatre fois à des recherches dans le N-SIS avec son propre nom de famille. Les autorités cantonales de protection des données, dans le cadre de leurs propres contrôles, ont également constaté que plusieurs utilisateurs cantonaux avaient procédé à des recherches dans le N-SIS avec leur propre nom de famille. Ces utilisateurs ont indiqué aux autorités cantonales de protection des données que ces recherches avaient été faites à des fins de formation. Nous avons estimé que le cas relevé lors de notre contrôle auprès du Corps des gardes-frontière entrait également dans cette catégorie. Pour cette raison, nous avons renoncé à prendre contact avec la personne concernée.

Le Groupe de coordination Schengen des autorités suisses de protection des données a préparé un courrier visant à sensibiliser les utilisateurs à respecter le cadre légal, notamment en ne recherchant pas dans le N-SIS des signalements relatifs à des personnes de leur famille ou entourage ni à des personnalités connues. Ce courrier indique également que le respect des normes légales doit également être garanti lors de cours de formation, en utilisant par exemple la plateforme dédiée. Chaque membre du Groupe de coordination peut faire usage de ce courrier dans le cadre de ses activités de sensibilisation respectivement de contrôle à son niveau de compétence fédérale ou cantonale. Dans le cadre de notre contrôle, nous avons adressé un tel courrier au Corps des gardes-frontière.

1.4.3 Mise en oeuvre Schengen: décision-cadre 2008/977/JAI

La transposition des obligations qui nous incombent en vertu de la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale a impliqué la révision de plusieurs lois fédérales. Les nouvelles dispositions de la LPD renforcent notamment l'indépendance de notre autorité.

La décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale constitue un développement de l'acquis de Schengen. À l'instar des autres États membres, nous avons dû prendre les mesures nécessaires pour nous conformer aux dispositions de la décision-cadre, ce jusqu'à fin novembre 2010.

La décision-cadre rappelle les principes généraux de licéité, proportionnalité, finalité et d'exactitude des données ainsi que les droits de la personne concernée et introduit certaines règles spécifiques. Elle définit en particulier les finalités pour lesquelles les données transmises par un État Schengen peuvent être traitées et fixe les conditions applicables lorsqu'une autorité d'un État Schengen envisage de transmettre à un État tiers, à une instance internationale ou à une personne privée des données reçues d'un autre État Schengen.

Même si les dispositions de la décision-cadre sont directement applicables, il a été nécessaire de réviser plusieurs législations: la loi fédérale sur la protection des données (LPD), la loi sur l'échange d'informations Schengen (LEIS), la loi fédérale sur les étrangers (LEtr), la loi sur l'asile (LAsi), la loi sur les armes (LArm), la loi sur les stupéfiants (LStup) et le code pénal (CP).

Les plus importantes modifications légales en matière de protection des données sont cependant contenues dans la LPD. La révision de la LPD, entrée en vigueur le 1er décembre 2010, entérine un renforcement de l'indépendance de notre autorité. Le préposé fédéral est désormais nommé par le Conseil fédéral pour une période de quatre ans avec approbation du Parlement. Par ailleurs, nous adressons nos rapports d'activités annuels à l'Assemblée fédérale et les transmettons simultanément au Conseil fédéral. Ceci met non seulement en œuvre les exigences de la décision-cadre, mais aussi les recommandations de l'UE adressées en 2008 lors de l'évaluation de la mise en œuvre de l'acquis Schengen en Suisse.

1.4.4 Méthodologie des contrôles coordonnés dans le cadre de Schengen

Les accords de Schengen prévoient la mise en place de contrôles des utilisateurs finaux du Système d'information Schengen (SIS). En raison de la structure fédérale de la Suisse, les compétences de contrôle sont partagées entre la Confédération et les cantons. Il est dès lors nécessaire d'avoir une méthode commune de contrôle.

Au niveau suisse, nous exerçons en collaboration avec les autorités cantonales de protection des données la surveillance des traitements des données effectués dans le cadre de l'utilisation du SIS. Nous coordonnons les tâches de surveillance avec les autorités cantonales, collaborons étroitement avec l'Autorité de contrôle commune Schengen dont nous sommes le point de contact national.

L'Autorité de contrôle commune décide parfois de déclencher des contrôles sollicitant des actions au niveau national. Les autorités suisses concernées sont alors appelées à exécuter un contrôle coordonné. Ce nouveau genre d'examen pose deux problèmes. L'un au niveau de l'uniformité des méthodes: Pour pouvoir coordonner et comparer les contrôles des différentes autorités de protection de données, il est nécessaire d'avoir une certaine uniformité. Le second problème relève de l'expérience dans les contrôles: Certaines autorités cantonales ne disposent en effet que de peu de ressources pour effectuer des contrôles et n'ont dès lors que peu d'expérience pour ce genre de tâche.

Pour résoudre ces problèmes et à la demande des cantons, le groupe de coordination des autorités suisses de protection des données a décidé le 12 novembre 2009 de créer un groupe de travail composé de représentants du PFPDT et de plusieurs autorités cantonales dont le but était de rédiger un document définissant la coordination et la méthodologie des contrôles.

Les résultats de ces travaux, finalisés sous forme d'un document décrivant les différents rôles ainsi que les étapes et processus de contrôles coordonnés, ont été présentés et adoptés lors de la séance du groupe de coordination du 16 septembre 2010 (cf. ch. 1.4.5 du présent rapport d'activité).

1.4.5 Groupe de coordination 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 œuvre 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 en application de la coopération Schengen.

Le groupe de coordination des autorités suisses de protection des données s'est réuni le 16 septembre 2010. Lors de cette réunion, nous avons informé les autorités cantonales de protection des données des principaux points abordés lors des réunions de l'Autorité de Contrôle Commune (ACC) Schengen et des activités de cette dernière. Nous avons également informé nos collègues cantonaux des résultats de nos contrôles effectués auprès du Corps des gardes-frontière ainsi qu'auprès du Consulat Suisse à Istanbul. À leur tour, les cantons ont présenté les résultats de leurs activités de contrôle auprès d'utilisateurs cantonaux du SIS (notamment BE, BS, FR et ZG). Au vu des résultats des différents contrôles effectués et des discussions du groupe de coordination nous avons constaté quelques cas d'utilisations abusives du SIS à des fins privées ou de formation. Afin d'y remédier, le groupe de coordination a décidé d'adresser un courrier de sensibilisation aux utilisateurs du SIS, tant au niveau fédéral que cantonal. Enfin, le groupe de coordination a examiné et adopté un document de méthodologie commune concernant les inspections coordonnées entre nos autorités respectives (cf. ch. 1.4.4 du présent rapport d'activité).

1.4.6 Projet de révision de la LMSI transmis au Parlement

Le Conseil fédéral a transmis au Parlement un projet de révision de la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI). Ce projet prévoit de remplacer le droit d'accès dit indirect par le droit d'accès direct selon les modalités visées aux articles 8 et 9 de la loi fédérale sur la protection des données (LPD).

Le Conseil fédéral a transmis au Parlement en octobre 2010 un projet de révision de la LMSI. En ce qui concerne le droit d'être renseigné, le projet soumis en consultation des offices prévoyait un droit d'accès direct basé sur la législation régissant l'accès aux systèmes d'information JANUS et GEWA. Le Conseil fédéral a fait un pas de plus en

prévoyant le droit d'accès direct en application des articles 8 et 9 de la LPD. Cette proposition constitue une avancée très importante pour les droits des personnes concernées. En effet celles-ci pourront avoir accès aux données les concernant et, le cas échéant, faire valoir leur droit de rectification.

Pour les autres points du projet, nous doutons toujours de la nécessité d'une révision de la LMSI. En effet, nous estimons que les instruments actuels de la LMSI, du Code pénal et de la procédure pénale sont suffisants pour atteindre les objectifs de sûreté visés. Dans le cadre de la consultation des offices, nous avons notamment demandé de renoncer à ancrer, au niveau de la loi, les dispositions contenues actuellement 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. Une telle extension représente une atteinte importante aux droits fondamentaux et doit ainsi respecter les principes de nécessité et de proportionnalité. Nous relevons, d'une part, que la législation en vigueur prévoit déjà l'obligation pour de nombreuses autorités de fournir des renseignements, respectivement le droit de communiquer des renseignements. D'autre part, le rapport chargé d'évaluer les résultats concrets de l'ordonnance susmentionnée n'a pas permis de démontrer la justification d'une extension du devoir de renseigner et du droit de communiquer au-delà de son seul effet théorique et psychologique. Les mesures proposées n'ayant pas atteint les objectifs visés, nous devons constater que les traitements de données personnelles correspondantes sont contraires au principe de proportionnalité. Nous saluons par contre le fait que les mesures les plus attentatoires à la sphère privée ne figurent plus, pour l'instant, dans le projet de révision de la LMSI transmis au Parlement.

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

En 2010, le nombre des demandes d'accès concernant le système d'information sécurité intérieure ISIS a été extraordinairement élevé. Cette vague de demandes a pour origine la publication en été 2010 du rapport de la Délégation des Commissions de gestion des Chambres fédérales concernant le traitement des données dans ISIS.

En 2010, 407 demandes d'accès appelées indirectes concernant ISIS ont été déposées auprès de notre secrétariat. Depuis 1998, c'est la deuxième année que le nombre de demandes dépasse très largement la moyenne (15 à 20 demandes par année). En 2008, 148 demandes avaient été déposées à la suite de cas concernant certains membres du Grand Conseil du canton de Bâle-Ville (cf. notre 16e rapport d'activités 2008/2009, ch. 1.4.4).

Le rapport de la Délégation des commissions de gestion des Chambres fédérales du 21 juin 2010 relatif au traitement des données dans ISIS exprime des doutes quant à l'exactitude et à la pertinence des données personnelles traitées et révèle de sérieux retards dans le contrôle qualité, voire l'absence même d'un tel contrôle. La publication du rapport et les réactions dans les médias ont mené à une augmentation massive du nombre des demandes d'accès dites indirectes concernant ISIS.

La Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) prévoit que nous adressons en principe une réponse standard par laquelle le requérant est informé que nous avons procédé à l'examen mais n'est pas informé s'il est enregistré ou non dans ISIS. Ce n'est qu'à titre exceptionnel que nous pouvons fournir de manière appropriée des renseignements aux personnes qui en font la demande, pour autant que cela ne constitue pas une menace pour la sûreté intérieure ou extérieure et qu'il n'existe pas d'autre moyen pour empêcher que ces personnes soient lésées gravement et de manière irréparable.

La situation décrite dans le rapport ainsi que les réactions et les commentaires dans les médias ont engendré une certaine insécurité chez plusieurs personnes. Nous avons examiné pour chaque demande de droit d'accès concernant ISIS si les conditions pour une information à titre exceptionnel étaient remplies en tenant compte de la situation particulière décrite ci-dessus. Nous avons pu faire usage de cette exception dans un grand nombre de cas. Dans ce cadre, nous avons été en contact avec le Service de renseignement de la Confédération. La grande majorité des personnes ayant déposé une demande d'accès ont reçu de notre part une réponse en décembre 2010 ou en janvier 2011. Les personnes qui ne sont pas satisfaites avec notre réponse peuvent encore exiger que la présidente de la Cour I du Tribunal administratif fédéral examine notre communication ou l'exécution de la recommandation que nous aurions le cas échéant émise.

1.4.8 Essai pilote du système d'information ISAS

Nous avons demandé au Service de renseignement de la Confédération (SRC) de préciser les banques de données qui sont touchées par l'essai pilote ainsi que de limiter le nombre de collaborateurs qui y participeront. Le SRC ayant fourni ces précisions, nous avons pu donner un avis favorable à cet essai pilote.

Avant de consulter les unités administratives concernées (consultation des offices), l'organe fédéral responsable de l'essai pilote doit nous communiquer de quelle manière il est prévu d'assurer que les exigences relatives à un tel essai sont remplies et doit nous inviter à prendre position. Dans le cas de l'essai pilote ISAS, le SRC ne nous a

pas informés avant la consultation des offices mais dans le cadre de celle-ci. Les dispositions réglant les modalités de traitement des données personnelles dans le cadre de l'essai pilote ISAS sont contenues dans l'ordonnance sur les systèmes d'information du SRC qui règle également le système ISIS. Cette solution de régir dans une même ordonnance un fichier (ISIS) qui est déjà entièrement opérationnel et un autre fichier en phase d'essai (ISAS) n'est à notre avis pas optimale. Il aurait été plus judicieux d'élaborer une ordonnance spécifique à l'essai pilote. Nous avons tout de même examiné si les exigences légales relative à une exploitation pilote étaient remplies.

Premièrement, les tâches qui nécessitent le traitement automatisé des données sensibles ou des profils de la personnalité doivent être réglées dans une loi au sens formel. La loi fédérale sur le renseignement civil (LFRC) prévoit que le SRC a pour tâches notamment de rechercher et d'évaluer à l'intention des départements fédéraux et du Conseil fédéral des informations sur l'étranger importantes en matière de politique de sécurité. Ces tâches nécessitent le traitement automatisé de données sensibles ou de profils de la personnalité. En effet, il n'est pas imaginable de traiter l'ensemble des données collectées autrement qu'en ayant recours à une procédure automatisée. Il est également clair que des données sensibles ou des profils de la personnalité seront traitées dans le cadre de la collecte de ces informations. La LFRC prévoit également, pour les tâches susmentionnées, le traitement de données personnelles, y compris les données sensibles et les profils de la personnalité. Nous avons ainsi constaté que la première condition était remplie.

Deuxièmement, des mesures appropriées doivent être prises afin de limiter les atteintes à la personnalité. L'ordonnance sur les systèmes d'information du SRC stipule que ce dernier fixe dans un règlement de traitement les mesures techniques et organisationnelles et la journalisation des traitements de données effectuées. Le droit d'accès au système d'information ISAS étant régi par les articles 8 et 9 de la loi fédérale sur la protection des données, les personnes concernées peuvent faire valoir leurs droits et cela sans restriction spécifique, notamment leur droit à la rectification ou à l'effacement. Le SRC nous a informés qu'un concept relatif à la protection des données et à l'information sera élaboré. Nous avons salué l'élaboration d'un tel document qui est utile dans le cadre des mesures destinées à la protection de la personnalité des personnes concernées. Par contre, afin de limiter les atteintes à la personnalité, seule une partie des données personnelles et des utilisateurs envisagés doit être inclue dans l'essai pilote. Dans le cas de l'essai pilote ISAS, il est suffisant que quelques banques de données soient mises en place et que seuls les collaborateurs responsables des domaines concernés puissent traiter les données. Sur notre intervention, le SRC a dû ultérieurement préciser quelles banques données, respectivement quels domaines, sont concernés par l'essai pilote et limiter le nombre de collaborateurs autorisés à traiter

les données personnelles. Nous avons constaté que la deuxième condition n'était dans un premier temps que partiellement remplie. Elle a été remplie quand le SRC a indiqué que seulement deux domaines sur six sont principalement concernés par l'essai pilote (terrorisme et non-prolifération) et que seulement 20% des collaborateurs du SRC participent à cet essai.

Troisièmement, la mise en œuvre du traitement doit rendre une phase d'essai avant l'entrée en vigueur d'une loi au sens formel indispensable. Selon les indications du SRC, de nombreuses questions techniques et organisationnelles liées aux futurs travaux du SRC ne pourront être réglées que dans le cadre de l'essai pilote ISAS. La question d'un éventuel accès restreint des autorités cantonales à ISAS sera également analysée. Il n'est pas exclu que les autorités cantonales en charge de la protection de l'État doivent accéder à un nombre restreint de données du fichier ISAS pour accomplir leurs tâches légales. L'efficacité d'un nouvel instrument mis en place pour procéder à l'analyse (en particulier le triage entre ISAS et ISIS) et à l'exploitation des informations entrantes doit nécessairement être vérifiée. Nous avons constaté que cette troisième condition était aussi remplie.

En conclusion, nous avons émis un avis favorable concernant l'essai pilote ISAS, sous réserve du respect de nos exigences (limitation des domaines ainsi que des collaborateurs).

Le SRC devra transmettre, au plus tard deux ans après la mise en œuvre de la phase d'essai, un rapport d'évaluation au Conseil fédéral. Nous avons demandé au SRC de nous transmettre un rapport intermédiaire concernant l'essai pilote ISAS.

1.4.9 Révision de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication

La loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) doit être adaptée à l'évolution technique et inclure explicitement l'Internet, donc le courrier électronique et la téléphonie par Internet. Dans le cadre de la consultation des offices relative à la révision de la LSCPT, nous avons fait part de nos propositions sur divers points.

Lors du premier projet de la LSCPT, nous avions déjà contesté le champ d'application de la loi, formulé de manière très générale. Bien que ce premier projet ait par la suite été modifié avant d'être mis en consultation, nous sommes d'avis que les commentaires contenus dans le rapport explicatif sont encore toujours formulées de manière trop générale.

En outre, nous estimons que le catalogue des délits impliquant l'utilisation de chevaux de Troie sur des ordinateurs ou autres petits appareils (p.ex. smartphones), tel qu'il est prévu dans le code de procédure pénale (CPP), est trop large, car il constitue une atteinte importante à la vie privée des personnes concernées. En effet, l'installation de tels logiciels espions permet de surveiller non seulement les télécommunications, mais l'ensemble de l'ordinateur. Ceci inclut l'accès à toutes les données enregistrées – y compris à des informations privées et à caractère intime – ainsi qu'aux modules d'enregistrement de données intégrés à l'appareil, tels que microphones ou caméras. Dans notre prise de position, nous avons demandé que ce catalogue soit limité aux délits majeurs. Malheureusement, cette demande n'a pas été prise en compte dans le projet de consultation.

Le projet de loi prévoit également un droit de consultation et d'accès pour les personnes surveillées. Les partenaires des télécommunications qui ne sont pas impliqués dans une procédure pénale ne sont par contre pas informés que des données les concernant sont enregistrées dans le cadre de telles mesures de surveillance. Nous sommes d'avis que le droit de consultation et d'accès doit également être accordé de manière simple aux personnes qui ne sont pas impliquées dans la procédure pénale.

Suite au jugement prononcé par le Tribunal constitutionnel fédéral allemand, selon lequel la conservation de données à titre préventif n'est admise plus qu'à des conditions très strictes, l'extension prévue de la durée de conservation des données accessoires de 6 à 12 mois devrait faire l'objet d'une nouvelle appréciation sous l'angle de la proportionnalité.

Nous approuvons en outre les dispositions en matière de protection des données qui doivent être mises en œuvre pour le système d'information exploité par le service de surveillance.

1.4.10 Traités d'entraide internationale en matière pénale avec l'Argentine et la Colombie

Lors de la consultation relative aux traités d'entraide internationale en matière pénale avec l'Argentine et avec la Colombie, nous avons rappelé l'application par la Suisse de la décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ainsi que des clauses types de protection des données pour les contrats bilatéraux en matière répressive adoptées par l'UE. Nous avons recommandé l'insertion d'une clause type énonçant les principes de protection des données dans les contrats bilatéraux en matière répressive conclus par la Suisse avec des États tiers à l'UE.

Lors de la consultation législative relative aux traités d'entraide internationale en matière pénale de la Suisse avec l'Argentine et avec la Colombie, nous avons constaté que ces traités ne contiennent pas de clause relative à la protection des données à caractère personnel. Nous avons rappelé en particulier l'application de la décision-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ainsi que des clauses types de protection des données pour les contrats bilatéraux en matière répressive adoptées par l'UE. Ces normes de protection des données ont été élaborées dans le cadre de la coopération au sein de l'espace de justice, liberté et sécurité en Europe, à laquelle la Suisse est associée. Elles servent également de référence lors de la conclusion de traités d'entraide internationale en matière pénale par la Suisse avec des États tiers à l'UE.

Nous avons souligné qu'il était essentiel de garantir un niveau de protection des données adéquat pour les données à caractère personnel traitées dans le cadre de l'entraide judiciaire en matière pénale. Ainsi, une clause type de protection des données dans les contrats bilatéraux en matière répressive permettrait un renvoi général à la législation interne des États parties en matière de protection des données. Elle permettrait, le cas échéant, de garantir l'application des principes de protection des données tels que prévus dans la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE 108) et la Recommandation 87/15 du Conseil de l'Europe visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police ainsi que dans la législation de l'UE aux données personnelles traitées dans ce cadre. Il s'agit en particulier de garantir la légitimité des traitements de données à caractère personnel, la limitation de leurs finalités et leur proportionnalité, l'actualité des données échangées ainsi que la sécurité et la confidentialité des transferts de ces données.

1.5 Santé

1.5.1 Révision totale de la loi sur les épidémies

Suite à de nombreuses remarques de notre part et à nos prises de position correspondantes, une base légale suffisante pour la protection des données a été créée lors de la révision totale de la loi sur les épidémies. Celle-ci inclut pour la première fois une réglementation de la protection transfrontière des données sensibles de patients.

Vu les nombreuses épidémies de ces dernières années (SARS, grippe aviaire, grippe pandémique H1N1), les fournisseurs de prestations (hôpitaux, EMS, médecins) ainsi que les entreprises de voyage et de transports aériens nous ont à diverses reprises demandé comment il fallait traiter, de manière conforme à la protection des données, les données sensibles de patient collectées dans le cadre d'une maladie menaçant de se transformer en épidémie. Nous avons alors réalisé que la protection des données pour les cas de maladies apparaissant de manière inattendue et souvent à une échelle mondiale ne disposait pas d'une base légale suffisante. C'est la raison pour laquelle nous avons à plusieurs reprises suggéré à l'Office fédéral de la santé publique (OFSP) de mettre à profit la révision prévue de la loi sur les épidémies pour s'assurer que celle-ci constitue une base légale suffisante. Nous avons pu apporter nos propositions de modification dans le cadre de la consultation des offices.

Comme nous avons pu constater à la lecture du message et du projet de la loi révisée sur la lutte contre les maladies transmissibles de l'homme (loi sur les épidémies), «définit le but visé par l'exploitation des données collectées, la durée de leur conservation ainsi que leur échange entre les autorités d'exécution et les médecins de même que d'autres institutions chargées du traitement de maladies transmissibles. Les possibilités et les limites de la communication d'informations aux autorités étrangères sont également inscrites dans la loi conformément aux principes de la protection des données.» Avec cette loi sur les épidémies entièrement révisée et son deuxième titre sur le traitement des données dans ce domaine sensible de la santé, la protection des données dispose pour la première fois d'une base légale suffisante.

1.5.2 Cybersanté (eHealth): importants concepts de détail

Cette année également, nous avons été confrontés à quelques défis en matière de protection des données dans le cadre du grand projet Cybersanté (eHealth) Suisse. D'importantes activités ont eu lieu, tant dans le domaine de l'informatique que du droit. Il convient de souligner ici le concept des rôles ainsi que la recommandation visant à régler sur le plan légal l'application de la stratégie en matière de cybersanté.

Les activités dans le domaine de la santé publique génèrent un volume important de données relatives aux patients. Vu qu'il s'agit en majorité d'informations relatives à l'état physique et psychique de ces derniers, il est nécessaire d'appliquer des prescriptions sévères en vue de protéger les droits de la personnalité des personnes concernées. Les points faibles qui ont été reconnus dans les processus ne doivent pas être repris dans le système Cybersanté, même s'il s'agit d'aspects appréciés. C'est pourquoi nous avons demandé aux divers acteurs de nous indiquer clairement de quelles informations ils ont besoin pour quelle tâche et quels sont les rôles qui peuvent le mieux couvrir les processus actuels et futurs. Ceci a donné lieu à un catalogue très varié de souhaits plus ou moins justifiés.

La question de savoir qui nécessite quoi, quand et de la part de qui a permis de classer les revendications des acteurs de la cybersanté. Les réponses nous ont permis de dégager les principes suivants pour la planification de la cybersanté ainsi que pour le travail dans son sein:

- Pour pouvoir participer à la cybersanté, les patients et le personnel soignant doivent avoir été authentifiés de manière univoque.
- Seules les données qui documentent ou confirment les connaissances nécessaires au traitement des patients sont significatives.
- Dans la cybersanté, chaque fonction est attribuée à un rôle qui à son tour définit le droit à un ensemble clairement délimité d'informations.
- Les informations contenues dans la cybersanté ne peuvent être publiées dans des registres qu'aussi longtemps qu'elles révèlent une importance pour les acteurs impliqués.

Les recommandations relatives au concept des rôles et aux métadonnées (Recommandations II «Normes et architecture») reflètent ces principes.

Le 30 septembre 2010, un groupe d'experts a remis au Département fédéral de l'intérieur son rapport intitulé «Mise en œuvre de la Stratégie Cybersanté (eHealth) Suisse: recommandations relatives à la réglementation légale». Dans notre prise de position,

nous avons fait remarquer, en ce qui concerne les mesures proposées à moyen terme, que nous doutions fortement que l'article 117 de la Constitution fédérale ne donne la compétence à la Confédération d'édicter également des exigences contraignantes concernant le dossier électronique du patient pour les institutions cantonales de droit public. La Confédération a à notre avis uniquement la compétence de régler l'assurance maladie et accidents. Le dossier électronique du patient représente cependant en premier lieu un outil permettant d'assurer le flux d'information tout au long de la chaîne de traitement du patient et non un outil pour la mise en œuvre de l'assurance-maladie. Pour autant que l'article 117 de la Constitution soit applicable, sa compétence de réglementation serait limitée au domaine de l'assurance-maladie obligatoire.

Nous avons également critiqué le système du «caractère doublement facultatif». Ce dernier prévoit que l'utilisation du dossier électronique du patient soit facultative aussi bien pour les patients que pour les prestataires de soins. Nous sommes convaincus que la vision et l'objectif de la stratégie Cybersanté prévoient clairement le droit à l'autodétermination en matière d'information. Cette dernière apparaît comme fil conducteur dans toutes les idées relatives à la mise en œuvre de la stratégie Cybersanté. Il appartient au patient de décider qui est autorisé à traiter quelles données le concernant. Le prestataire de soins peut donc proposer de consigner dans le dossier électronique du patient une information importante pour le traitement et il ne peut pas refuser une proposition analogue de la part du patient. Le droit à l'autodétermination en matière d'information du patient ne peut donc pas être restreint par le personnel soignant, à moins qu'une loi au sens formel le prévoie.

1.5.3 Insécurité autour de la carte d'assuré

La remise par les assureurs-maladie de la carte d'assuré augmente la confusion dans la population. De plus en plus de patients s'adressent à nous.

Au cours de l'année sous revue, quatre assureurs ont commencé à envoyer la carte d'assuré à leurs clients, accompagnée d'un «mode d'emploi» et des conditions d'utilisation. Pourtant, ni la carte, ni les documents informatifs annexés n'ont apporté vraiment plus de clarté. Bien que les organismes compétents tels que l'Office fédéral de la santé publique aient régulièrement donné des informations sur la carte d'assuré, les patients sont désécurisés et nombre d'entre eux s'adressent à nous. Leur souci principal est que la «carte santé» permette aux caisses-maladie d'accéder aux données de santé des personnes assurées. Ceci n'est bien sûr pas prévu par la loi, mais comme chaque caisse-maladie possède et distribue sa propre carte d'assuré, aucune garantie ne peut finalement être donnée quant au contenu et à la fonction de la carte.

Un sujet qui a également soulevé des questions est la procédure de consentement pour la communication d'indications concernant une éventuelle assurance complémentaire lors de la consultation en ligne. L'ordonnance relative à la carte d'assuré prévoit que cette demande ne peut avoir lieu qu'avec le consentement de l'assuré. Pour des raisons de simplification, les assureurs ont choisi le système de l'option de retrait (opt-out): L'assuré doit communiquer par écrit à son assureur s'il ne souhaite pas d'indication concernant une assurance complémentaire au cours de la consultation en ligne. Une telle procédure n'est à notre avis pas très respectueuse de la protection des données. Les caisses-maladie avancent cependant l'argument compréhensible que le nombre de personnes qui ne désirent pas accorder l'accès aux informations concernant l'assurance complémentaire est si faible qu'il ne justifierait pas les frais supplémentaires de mise en place d'un système «opt-in».

Dans l'ensemble, la carte d'assuré reste un sujet à suivre de manière critique sous l'angle de la protection des données. Il reste à espérer que l'évolution du projet Cybersanté permettra à la carte d'assuré de devenir un instrument utile qui soit également compris par les assurés.

1.5.4 Exposé sur le traitement de données de patients devant le Conseil de l'Europe à Strasbourg

Le Conseil de l'Europe nous a invités à faire un exposé sur le traitement de données de patient dans le cadre d'une réunion du Comité directeur pour la Bioéthique du Conseil de l'Europe. La question centrale était de savoir s'il est nécessaire d'avoir des réglementations et si oui, lesquelles. Nous avons réussi à démontrer qu'un traitement de données de santé qui ne s'appuie pas sur des règles valables ne peut pas être bénéfique pour un système de santé national.

Les données de santé suscitent un grand intérêt et diverses institutions font valoir leurs revendications à des fins diverses. Ces revendications peuvent se concurrencer et ne sont pas toujours pour le bien des patients. Lorsqu'il s'agit d'examiner la nécessité d'avoir une réglementation, deux éléments sont décisifs: le premier est la motivation qui se cache derrière ces prétentions; le deuxième concerne le niveau de détail des données de santé qui est nécessaire pour répondre aux revendications respectives.

La motivation se cachant derrière les prétentions peut être de nature médicale ou de nature non médicale. Le motif de nature médicale vise principalement à déceler et éviter des dommages menaçant la santé d'individus ou de groupe de personnes. Le motif de nature non médicale est de développer des produits, procédés ou systèmes qui permettent ou appuient les activités dans l'intérêt de la santé de l'individu. Bien qu'il

soit difficile de différencier les deux motifs, la plupart des institutions de la santé publique en Suisse peuvent être associées au moins à un des deux motifs. Ainsi, un médecin qui diagnostique une grippe chez un patient et la traite, agit selon un motif de nature médicale. L'entreprise informatique qui développe et commercialise un système pour la gestion de données patient est incitée par un motif de nature non médicale. Un assureur appartient en principe au deuxième groupe, étant donné qu'il ne dispense pas de soins médicaux à ses patients, mais se charge d'assurer le financement des prestations. Il faut cependant relever que de plus en plus d'assureurs estiment qu'ils sont en droit d'influencer de manière directe la nature des traitements dans le but d'optimiser les coûts. Cet exemple montre qu'une même institution peut manifester un intérêt pour des données de santé aussi bien pour un motif médical que non médical.

Quant au deuxième élément, celui du niveau de détail (et donc du volume) des données de santé, il est bien plus difficile à cerner. Les revendications justifiées s'accompagnent souvent de convoitises superflues. En plus des données nécessaires pour un but précis, on s'efforce d'accumuler une montagne de données non essentielles et superflues, souvent pour une seule raison: devoir réduire les données au strict minimum nécessaire demande plus d'effort et signifie une perte de prestige. La personne qui traite les données, que ce soit un membre du personnel soignant, une entreprise informatique ou un assureur-maladie, est tenue de se restreindre au minimum absolu des données dont elle a besoin pour atteindre le but poursuivi. Cette restriction doit cependant être compréhensible aussi bien pour celui qui traite les données que pour le patient et elle ne doit pas pouvoir être appliquée de manière arbitraire.

Si la société n'est pas prête à accepter que l'accès aux données de santé ne soit accordé qu'à ceux qui le demandent avec suffisamment d'insistance, elle doit édicter des règles contraignantes relatives aux droits et aux obligations lors du traitement des données de santé.

1.5.5 Implications de la vente de médicaments par correspondance sur la protection des données

Un examen des faits auprès de deux pharmacies de vente par correspondance a montré que les entreprises contrôlées avaient une bonne approche des principes de la protection des données et que les mesures nécessaires à la protection des données des patients étaient prises. Par contre, des incertitudes demeurent quant aux données médicales que ces entreprises sont obligées de traiter.

Au cours de l'année sous revue, nous avons effectué un examen des faits auprès de deux pharmacies de vente par correspondance. L'une de ces procédures a été close,

la seconde le sera bientôt. Dans les deux cas, nous avons toutefois constaté que les entreprises en question sont conscientes du caractère sensible des données personnelles qu'elles traitent et qu'elles ont pris les mesures nécessaires à la garantie de la protection et de la sécurité de ces données. Nous avons noté en particulier que les deux entreprises procèdent à une séparation claire entre données administratives et données médicales. Ainsi, les collaborateurs n'ont accès aux données médicales que s'ils en ont absolument besoin. Par contre, nous avons constaté que des incertitudes demeurent en ce qui concerne les données médicales devant être absolument traitées conformément aux dispositions légales sur la qualité et la sécurité. Cette question est déterminante pour l'appréciation du devoir de déclaration d'un fichier dans notre registre accessible au public (www. datareg.admin.ch).

1.5.6 DVD d'une clinique privée contenant des prises de vue de plusieurs opérations

Une clinique privée a remis par inadvertance à un patient un DVD ne contenant pas seulement des prises de vue le concernant, mais aussi celles de 17 autres patients. Ces images étaient accompagnées de données complémentaires comme le nom du patient filmé, le chirurgien ayant opéré, le genre et la date de l'intervention.

Le proche parent d'un patient opéré dans une clinique privée nous a informés par écrit qu'un DVD avait été remis à ce patient avec non seulement des données concernant son opération, mais aussi celles de 17 autres patients. Il nous a envoyé ce DVD. En raison de la violation grave de la protection des données, nous avons immédiatement procédé à un examen des faits sur place.

L'examen des faits et plus particulièrement nos recherches sur place nous ont permis de constater que la violation des dispositions sur la protection des données était due à une erreur de manipulation involontaire des données concernant les opérations par le personnel soignant en charge de la vidéo dans la salle d'opération. Un collaborateur de l'hôpital avait involontairement sélectionné toutes les données enregistrées sur le chariot-vidéo et les avait copiées sur le DVD remis au patient après l'opération. L'examen des faits sur place nous a permis de constater que ce genre d'erreur peut très aisément arriver du fait de l'interface d'utilisateur du système vidéo. A la suite de cet incident, la clinique a fait suivre une formation spécifique à tous ses collaborateurs travaillant aux chariots-vidéo et a attiré expressément leur attention sur le danger d'une sélection non intentionnelle de fichiers-images. Sur notre initiative, la clinique a en outre informé tous les patients et les patientes touchés par cette erreur de manipulation.

La clinique ayant déjà pris toutes les mesures visant à empêcher d'autres violations des dispositions de protection des données, nous avons décidé de ne pas faire de recommandation. Cet incident montre cependant que nous sommes encore loin de la sécurisation des systèmes de traitement de données dès leur conception (security by design). Ceci est particulièrement inquiétant si l'on considère que ces installations-vidéo sont utilisées dans de nombreuses cliniques de Suisse.

1.5.7 Sous-traitance (outsourcing) malgré le secret médical?

Conformément à la loi sur la protection des données, un traitement de données peut être confié à un tiers à condition qu'aucune obligation légale de garder le secret ne l'interdise. Dans le domaine médical en particulier, la question se pose de savoir si le secret concernant les données des patients autorise que le traitement soit confié à un tiers.

Le secret médical, inscrit dans le code pénal suisse, constitue une obligation légale de discrétion. Malgré cela, il est d'usage courant dans les cabinets médicaux et dans les cliniques de confier les traitements de données à des tiers. Nous avons d'abord analysé les bases légales, puis avons prié l'Office fédéral de la justice (OFJ) de rendre un avis de droit sur la question.

Selon l'OFJ, les personnes chargées par les médecins ou les cliniques de traiter les données doivent être considérées comme du personnel auxiliaire. Donc, selon cette approche, il ne s'agit pas du tout ici d'un traitement de données confié à un tiers au sens de la loi fédérale sur la protection des données. De ce fait, le secret médical n'est pas mis en cause et la transmission du traitement des données au personnel auxiliaire ne nécessite pas le consentement du patient. Dans sa prise de position, l'OFJ définit néanmoins les conditions dans lesquelles la personne mandatée peut être considérée comme auxiliaire: elle doit être choisie avec soin, être instruite en conséquence et on doit pouvoir procéder concrètement à une surveillance et établir des directives. Si ces conditions sont remplies, la personne mandatée peut être considérée comme auxiliaire.

Pour nous, cette position est problématique et risquée pour les médecins ou les cliniques. Elle a pour conséquence que les collaborateurs d'une entreprise devraient être considérés comme auxiliaires du médecin alors que selon toute probabilité, le médecin ne connaît absolument pas ces personnes. Il faut partir de l'idée que les personnes morales ne peuvent être considérées comme auxiliaires. Nous conseillons donc aux médecins et aux cliniques de demander aux patients leur consentement avant de confier le traitement de leurs données à un tiers.

1.5.8 Exigences envers un registre des diagnostics

La Confédération prévoit de créer une base légale pour un registre des diagnostics qui, dans un premier temps, devrait contenir les diagnostics du cancer. La planification d'un tel registre doit répondre à des exigences très élevées en matière de protection des données. Nous nous sommes engagés en conséquence dans le groupe de travail.

Nous avons participé ces deux dernières années à un groupe de travail qui avait pour tâche d'examiner la création des bases légales fédérales nécessaires à la tenue d'un registre des diagnostics par la Confédération.

Il s'agirait dans un premier temps d'enregistrer surtout les affections cancéreuses. La situation au niveau des législations cantonales dans ce domaine est actuellement très hétérogène. Seuls les registres du cancer des cantons du Tessin, du Jura et de Lucerne peuvent s'appuyer sur une base légale. Il existe pourtant, selon l'Office fédéral de la santé publique (OFSP), actuellement 11 registres cantonaux ou régionaux qui couvrent 22 cantons. Tous ces registres disposent d'une autorisation générale de la Commission d'experts du secret professionnel en matière de recherche médicale.

Les registres qui recensent tous les nouveaux cas d'une maladie donnée ainsi que leur évolution pour l'ensemble de la zone géographique concernée permettent d'une part d'obtenir des indications fiables sur la fréquence des maladies recensées et de l'évolution de celle-ci dans le temps ainsi que sur l'évolution des profils de risque (combinaison des facteurs de risque à l'origine de la maladie). D'autre part, ils constituent pour certaines maladies la base d'informations qui permet de définir des indicateurs de qualité. De tels registres permettent pour les maladies chroniques, qui demandent un traitement et un suivi impliquant divers prestataires, en particulier pour le cancer, de se faire une idée de la qualité de toute la chaîne de traitement. C'est la raison pour laquelle on a fixé dans ces travaux la nécessité de communiquer obligatoirement un ensemble de données minimum afin d'obtenir le taux de saisie visé, à savoir 90 % des nouveaux cas diagnostiqués.

La création d'un registre des diagnostics représente un gros défi du point de vue de la protection des données; nous nous sommes donc engagés en conséquence dans le groupe de travail. La personnalité des personnes concernées doit être bien protégée et prise en compte lors de la conception technique.

Nous avons également eu la possibilité, dans le cadre de la consultation des offices concernant la requête au Conseil fédéral sur le recensement des diagnostics de cancer et autres, de donner notre avis. Nous y avons défendu le point de vue que la décision concernant l'admission d'autres diagnostics incombe au législateur. Ce n'est qu'en

impliquant tous les représentants de milieux intéressés que nous considérons le discours politique comme assuré et les restrictions des droits de la personnalité comme démocratiquement légitimisées Cet aspect est pour nous essentiel.

Un autre aspect sur lequel nous nous sommes prononcés est celui de la finalité, qui doit être formulée très soigneusement. Nous nous opposons à une formulation trop générale: Plus une finalité est formulée de manière générale dans un texte de loi, plus le nombre de traitements de données possibles est élevé sans que ceci soit clairement apparent pour les personnes concernées.

L'ensemble de données minimum qui doit obligatoirement être communiqué doit être aussi restreint que possible. A ce sujet, nous défendons le point de vue qu'il y a lieu d'utiliser une approche basée sur les rôles: l'ensemble de données minimum doit être différent selon le fournisseur de prestations (laboratoire, médecin, hôpital, etc.).

Le 3 décembre 2010, le Conseil fédéral a mandaté le Département fédéral de l'intérieur d'élaborer un avant-projet de cette loi d'ici au printemps 2012. Nous continuerons à suivre attentivement ces travaux pour prendre position le cas échéant.

1.5.9 Contrôle d'un registre du cancer

Même dans les cas où un registre du cancer dispose d'une autorisation générale de la Commission d'experts, le médecin doit demander le consentement des patients atteints du cancer, dans la mesure où cela est possible et raisonnablement exigible. Ce n'est que dans les cas où le patient ne peut plus être contacté ou qu'il ne serait pas raisonnable de lui demander son consentement que le médecin qui communique les données au registre du cancer peut s'appuyer sur l'autorisation générale de la Commission d'experts. Lors d'un contrôle du registre, nous avons en outre pu constater que seule une partie des processus d'exécution des tâches étaient documentés et que les mesures pour la sécurité des données n'étaient pas toutes conformes à l'état actuel de la technique.

Lors du contrôle d'un registre du cancer, nous avons constaté que les exploitants avaient admis par erreur que l'autorisation générale de la Commission d'experts leur permettait de collecter les données personnelles des patients atteints de cancer sans le consentement de ces derniers. Ceci n'est cependant pas conforme aux exigences normatives. Le médecin traitant doit informer le patient sur les activités de recherche pour lui demander, après un délai de réflexion, son consentement. Si le patient ne répond pas à une demande correspondante, ceci peut être interprété comme consentement tacite. Lorsque les patients concernés ne peuvent pas être contactés

personnellement notamment parce qu'on a perdu leur trace ou que leur nombre est trop important, il faut partir du principe que la demande du consentement ne soit pas possible ou raisonnablement exigible. Dans ces cas, ne subsiste que le devoir d'information mentionné qui consiste à informer sur la possibilité de faire opposition à l'utilisation des données à des fins de recherche. Dans de tels cas, le registre du cancer (ou le médecin traitant pour la communication des données du patient au registre du cancer) peut invoquer l'autorisation générale de la Commission d'experts du secret professionnel en matière de recherche médicale et utiliser les données de ces patients à des fins de recherche, pour autant que ces derniers n'y aient pas opposé leur veto. La Commission d'experts a pris position à ce sujet dans son rapport d'activités pour les années 2001 à 2004 sous le titre «Risque de confusion entre le devoir d'information et le devoir de rechercher le consentement» (voir www.ofsp.admin.ch).

Nous avons également fait remarquer que le consentement des patients atteints du cancer n'était légalement valable que si ces derniers peuvent reconnaître comment leurs données seront traitées. L'information à ce sujet doit donc être faite de manière bien compréhensible. Ainsi, le patient concerné doit être informé sur la manière dont ses données sont collectées et pseudonymisées avant d'être utilisées sous forme anonymisée pour les travaux de recherche. De plus, la personne concernée doit être informée que la mise en relation avec les autres registres du cancer est faite avec les données d'identification. Il serait cependant aussi possible d'attribuer les données à l'aide de procédés de pseudonymisation. Nous avons déjà mentionné cette possibilité dans nos précédents rapports d'activités. Dans les cas où un projet de recherche ne peut pas être effectué avec des données anonymes, p. ex. parce qu'il est nécessaire d'obtenir des données complémentaires de la part du patient concerné, il est nécessaire d'obtenir le consentement des personnes concernées pour pouvoir poursuivre ce projet. Pour qu'ils puissent signer une déclaration de consentement légalement valable, les patients concernés doivent recevoir au moins les informations suivantes: le nom de la personne responsable du projet de recherche, la finalité, les modalités du traitement de données, le cercle des personnes qui obtient des informations personnelles ainsi que la date d'anonymisation ou de destruction des données.

De plus, les patients concernés doivent être informés sur leur droit à révoquer leur consentement et à demander d'obtenir des informations sur les données les concernant ou de pouvoir les consulter. Nous avons également demandé que les processus, depuis la collecte des données personnelles jusqu'à leur anonymisation ou destruction, soient documentés. Sinon, il ne serait pas possible de comprendre le déroulement des tâches et les étapes du traitement des données (manque de transparence).

Il est pour le traitement de données personnelles sensibles nécessaire de mettre en œuvre des mesures de sécurité correspondant à l'état actuel de la technique. Dans ce domaine, nous avons constaté que les données transmises par voie électronique ne sont pas toujours chiffrées ou le sont selon un procédé de chiffrement qui n'est pas suffisamment sûr. De plus, nous avons également indiqué que les données personnelles (données identifiantes) doivent être stockées sous forme cryptée sur les supports de données (notamment sur les disques durs) et que la procédure de connexion au système en ligne doit effectuer une authentification à deux facteurs, p. ex. en requérant aussi bien une carte à puce (possession) qu'un code personnel (connaissance). De plus, il est utile d'afficher à l'écran la date et l'heure de la dernière connexion afin de permettre à l'utilisateur de constater si quelqu'un d'autre a utilisé son compte entre-temps.

En ce qui concerne la journalisation, nous avons constaté que celle-ci n'était pas effectuée de manière assez complète. L'objectif de cette dernière est de pouvoir garantir la reconstitution des traitements de données personnelles. Du point de vue de la protection des données, il s'agit principalement de savoir qui a traité quelles données personnelles, à quel moment, de quelle manière et à quelles fins. Les données consignées doivent en outre être enregistrées sous une forme qui permet de les analyser à l'aide d'outils. On veillera également à ce que la journalisation soit effectuée de manière aussi pseudonymisée que possible et qu'elle satisfasse aux exigences de la révision.

1.5.10 Recherche et protection des données

Nous avons participé à Bruxelles à une conférence sur le thème de la protection des données dans la recherche médicale. Nous serons confrontés dans ce domaine à de nouveaux défis ces prochaines années.

Très souvent, l'environnement international des projets de recherche confronte les responsables de projet à des exigences complexes du point de vue juridique. Au cours de l'année sous revue, nous avons à nouveau conseillé diverses entreprises dans l'application des exigences de protection des données dans ce domaine.

En novembre, nous avons participé à la conférence internationale «Privacy and Scientific Research: from obstruction to construction» à Bruxelles. La conférence a été organisée par l'autorité de protection des données belge, du fait que la Belgique assure actuellement la présidence du Conseil de l'Union européenne. Le programme était axé sur deux préoccupations majeures: la protection des données, d'une part dans la recherche médicale, d'autre part dans la recherche historique. Nous nous sommes

concentrés sur les thèmes touchant à la recherche médicale, étant donné qu'en Suisse la recherche historique est principalement faite par les universités, lesquelles relèvent de la compétence des autorités de protection des données cantonales.

Dans les groupes de travail, quelques représentants de l'industrie pharmaceutique ont souhaité une certaine uniformisation dans l'application des directives de protection des données de l'UE, du moins pour l'espace européen, par exemple pour la réalisation d'essais cliniques. Ils ont également critiqué la qualité très variable des prestations de conseil fournies par les autorités locales de protection des données.

Les exposés sur la recherche en matière de génétique ont suscité beaucoup d'intérêt. Les développements dans ce domaine sont énormes alors que les coûts des examens génétiques sont en constante diminution. Ceci crée de nouveaux défis pour la protection des données.

La conférence a pris fin avec des recommandations à l'adresse des autorités législatives, des chercheurs, des archives et des autorités de protection des données. Les autorités législatives ont été appelées à harmoniser sur le plan international les notions d'identité, d'anonymat et d'identification, en faisant remarquer que le concept d'anonymat absolu ne faisait aucun sens dans la recherche médicale.

Les chercheurs devraient quant à eux s'informer sur la manière de traiter les données personnelles dans le domaine médical d'une manière qui soit conforme aux exigences de la protection des données et, si nécessaire, à se faire conseiller par les autorités de protection des données. Ces dernières ont été appelées à coordonner leurs activités avec celles des commissions d'éthique.

Il ne s'agit là que de quelques remarques sur cette conférence où nous avons également reçu des conseils pratiques. La documentation de cette conférence a été publiée sur Internet à l'adresse suivante: www.privacyandresearch.be

1.5.11 Protection des données dans le domaine de la recherche généalogique

Un projet de recherche prévoit d'établir la généalogie de personnes atteintes d'une maladie génétique orpheline. Nous avons attiré l'attention des responsables du projet sur certains points problématiques à prendre en compte du point de vue de la protection des données.

Nous avons été consultés à des fins de conseil sur un projet de recherche prévoyant d'établir la généalogie de personnes atteintes d'une maladie génétique orpheline. Ce dernier a pour but de rechercher les parents d'un patient souffrant d'une malade génétique orpheline par le biais d'une recherche généalogique afin d'informer ceux-ci

d'éventuels risques pour leur santé. Cette maladie est difficilement diagnosticable mais peut cependant être traitée médicamenteusement. L'espérance de vie des personnes atteintes de cette maladie diminue considérablement en l'absence de traitement. La loi fédérale sur la protection des données prévoit que le maître du fichier a l'obligation d'informer les personnes concernées de toute collecte de données sensibles. Or le fait que la société responsable du projet établisse l'arbre généalogique d'un patient d'une maladie génétique et que les membres de la famille sont potentiellement porteurs de cette maladie rend ces données sensibles. Dans ce cas, les personnes doivent être informées au plus tard lors de l'enregistrement des données ou, en l'absence d'un enregistrement, lors de la première communication des données à un tiers. Le projet en question ne prévoit cependant une information par lettre circulaire qu'une fois le projet arrivé à terme, soit après le moment prévu par la loi. Cela entraîne en outre un conflit avec le droit d'une personne à ne pas être informée sur sa propre constitution génétique prévu par la loi fédérale sur l'analyse génétique humaine. En effet, une telle prise de connaissance peut avoir des conséquences gravissimes sur l'état de santé psychique de la personne et influencer sa manière de vivre et son plan de vie durablement.

Nous avons sensibilisé le responsable du projet à cette problématique et allons continuer à accompagner ce projet.

1.6 Assurances

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

Les assurances-véhicules à moteur exploitent une plate-forme électronique de données afin de lutter contre la fraude à l'assurance. Nous avons examiné cette plate-forme et constaté que le système était en principe conçu dans le respect de la protection des données. Nous élaborons des solutions pratiques avec les personnes concernées sur les points où des améliorations sont encore nécessaires.

Le «Car Claims Information Pool» (CC-Info) est une plateforme d'échange électronique de données. Il a pour but la lutte contre la fraude à l'assurance dans le domaine des assurances-véhicules à moteur. CC-Info a été mis au point par une compagnie proche de l'Association suisse des assurances. Plusieurs grandes assurances-véhicules moteurs participent à ce pool d'information. La mise en œuvre informatique a lieu au centre de calcul de la Bedag Informatik SA à Berne, les assurances participant au projet ayant accès aux données par Internet.

Nous avons soumis le traitement des données effectué dans le cadre du pool CC-Info à un examen approfondi et avons constaté avec satisfaction que tous les participants faisaient preuve d'une compréhension adéquate des intérêts de la protection des données et, en particulier, avaient pris les mesures appropriées du point de vue technique et organisationnel.

Nous demeurons en contact avec les participants afin de trouver ensemble des réponses judicieuses et adéquates sur des points de détail pouvant être améliorés.

1.6.2 Enregistrements-vidéo dans les transports publics: transmission à des assureurs responsabilité civile

Les caméras désormais installées dans de nombreux transports publics ont pour but de protéger les voyageurs, l'exploitation et les infrastructures. Les données collectées à cette occasion éveillent de nombreuses convoitises. Toutefois, le cadre juridique pose ici des limites claires.

Un assureur-responsabilité civile engagé auprès de nombreuses entreprises de transport public nous a consultés pour savoir si les entreprises pouvaient lui permettre de consulter les enregistrements des installations-vidéo montées dans les véhicules afin d'évaluer les responsabilités dans les cas d'accidents de voyageurs.

La réglementation légale de la surveillance-vidéo dans les moyens de transport public est concrétisée dans la loi sur les chemins de fer, dans la loi fédérale sur le transport des voyageurs et plus particulièrement dans l'ordonnance sur la vidéosurveillance dans les transports publics. Bien que les règles qui figurent dans ces textes soient en principe exhaustives et priment en tant que normes spéciales sur les normes plus générales éventuellement divergentes, il convient de les interpréter à la lumière des principes de la loi sur la protection des données.

Les données personnelles ne doivent être traitées que dans le but qui était à l'origine de leur collecte, qui ressort des circonstances ou qui est prévu par une loi. Ces conditions devraient garantir que dès la collecte des données, la personne concernée puisse savoir comment et pourquoi les données la concernant sont traitées. C'est pour elle le seul moyen de décider si elle entend se soumettre à ce traitement; ce n'est qu'ainsi qu'elle peut exercer de manière efficace son droit fondamental de disposer librement des informations la concernant.

Le législateur a établi que la vidéosurveillance dans les moyens de transport public est licite afin de protéger les voyageurs, l'exploitation et les infrastructures. L'appréciation des prétentions en matière de responsabilité civile découlant d'accidents de voyageurs n'est donc pas incluse dans ces objectifs et par conséquent, la réglementation légale ne prévoit pas non plus que l'on puisse communiquer des enregistrements-vidéo à des tiers privés (par ex. une assurance-responsabilité civile). L'accès à ces enregistrements ne peut être accordé qu'aux autorités de poursuite pénale et aux autorités devant lesquelles les entreprises portent plainte ou font valoir des droits, si cette communication est requise pour les besoins de la procédure. Quiconque utilise ou communique des enregistrements-vidéo en violation de ces prescriptions est même punissable.

Selon le droit en vigueur, il est donc illicite pour une entreprise de transports publics de remettre des enregistrements-vidéo à son assureur-responsabilité civile. En revanche, les enregistrements peuvent être communiqués aux autorités compétentes (plus précisément les tribunaux) dans les procédures en vue de faire valoir (ou de rejeter) des prétentions en droit et dans le cadre du droit procédural applicable.

Un autre compte rendu sur la vidéosurveillance dans les transports publics se trouve au ch. 1.2.3 du présent rapport d'activités.

1.6.3 Usage abusif de données clients par des assurances maladie à des fins de marketing

Plusieurs assurances-maladie se sont adressées directement par courrier à certains assurés qui prenaient des médicaments spécifiques, afin de leur proposer des médicaments similaires, mais moins chers. Au vu de la pression croissante des coûts dans le domaine de la santé, on peut certes comprendre ce procédé; il n'en constitue pas moins une violation des dispositions de protection des données.

À la suite d'informations transmises par le représentant légal d'un laboratoire pharmaceutique, nous avons procédé à un examen des faits concernant plusieurs assurances-maladie. Il leur était reproché d'utiliser les données personnelles d'assurés soumis à un certain traitement et de leur écrire pour leur proposer des médicaments moins chers pouvant aussi être adaptés à leur cas.

Les caisses-maladie actives dans le domaine de l'assurance maladie obligatoire sont considérées comme des organes fédéraux car elles accomplissent une tâche publique de la Confédération. Elles sont donc soumises au principe de la légalité et ne doivent traiter les données personnelles que si ce traitement repose sur une base légale. Elles ne sont habilitées à traiter les données sensibles que si une loi au sens formel le prévoit expressément. La loi fédérale sur l'assurance-maladie détermine les buts dans lesquels les données personnelles des assurés (y compris les données sensibles) peuvent être traitées. La publicité pour des médicaments n'est pas comprise dans les buts de traitements prévus par la loi et constitue ainsi une violation des dispositions en matière de protection des données.

Suite à cette intervention, presque toutes les assurances-maladie qui avaient mené ce type d'actions de marketing les ont abandonnées. Avec une caisse-maladie, nous avons dû organiser une entrevue explicative en présence des responsables de l'Office fédéral de la santé publique. Ultérieurement, cette caisse a aussi abandonné ces pratiques.

1.7 Secteur du travail

1.7.1 Centralisation des ressources humaines à l'étranger

Les entreprises internationales sont de plus en plus nombreuses à centraliser leurs divisions des ressources humaines. Leurs filiales suisses se voient ainsi de plus en plus souvent priées de communiquer les données personnelles concernant leurs employés à la société-mère qui se trouve à l'étranger.

Beaucoup d'entreprises internationales ont aujourd'hui tendance à n'avoir qu'un seul service du personnel ou, pour le moins, à confier certaines parties de l'administration de leur personnel à un service central. De nombreux collaborateurs chargés de l'administration du personnel dans les filiales suisses ont été confrontés à ce nouvel état de fait et nous ont demandé si et à quelles conditions la transmission de données personnelles à l'étranger est autorisée.

La communication de données personnelles d'une filiale à la société-mère constitue une communication de données à une tierce personne et il faut, dans ce cas, que les règles de la loi fédérale sur la protection des données relatives à la communication transfrontière de données personnelles soient respectées. Selon l'emplacement de la société-mère, la communication de données à partir de la Suisse doit faire l'objet de différentes mesures. Lorsque les données sont envoyées aux États-Unis (ce qui était souvent le cas dans les demandes qui nous ont été adressées), l'une des trois conditions suivantes doit être remplie car les États-Unis ne garantissent pas une protection des données suffisantes: soit l'entreprise réceptionnant les données s'est enregistrée auprès du Département américain du Commerce conformément à l'accord Suisse/États-Unis établissant une sphère de sécurité en matière de protection des données («US-Swiss Safe Harbor Framework»), soit un contrat garantissant une protection des données adéquate a été conclu, soit les personnes concernées ont donné leur accord. Si l'entreprise en question se trouve dans un État garantissant un niveau adéquat de protection des données, la communication des données à partir de la Suisse peut se faire sans ces mesures. Le principe de transparence est toutefois aussi applicable dans ce cas. Les employés de la filiale suisse doivent être informés de la communication à l'étranger de données les concernant.

1.7.2 Système de reconnaissance biométrique pour les collaborateurs

Une entreprise a introduit un nouveau système de badge avec reconnaissance biométrique basé sur les empreintes digitales. D'une part le badge sert au contrôle de l'accès aux locaux, d'autre part il doit permettre l'accès à toutes les applications informatiques protégées par un mot de passe. Nous nous sommes rendus sur place pour examiner le système, qui se trouve actuellement en phase pilote, et avons constaté qu'il répond aux exigences posées par la protection des données.

L'entreprise, qui possède plusieurs milliers d'employés, occupe des locaux classés en diverses catégories; certains sont des secteurs de haute sécurité dont l'accès ne devrait être autorisé qu'à un petit nombre de collaborateurs. Le système de badge utilisé jusqu'ici (carte RFID avec impression de la photographie du visage) constituait certes un contrôle fiable de l'accès, mais au prix de beaucoup de ressources. L'entreprise a donc mis au point une solution permettant de vérifier de manière fiable les personnes disposant de l'autorisation d'accès avec un minimum d'efforts. Leur choix s'est porté sur un système de reconnaissance biométrique permettant une vérification automatisée et extrêmement sûre.

Lors du contrôle d'accès, le modèle (template) de l'empreinte digitale est crypté après la lecture et ensuite scindé en deux. Une partie est stockée de manière centralisée et la seconde est déposée de manière décentralisée sur le badge (une carte RFID). Ces deux parties ne peuvent être utilisées séparément: les données stockées de manière centralisée ne peuvent être utilisées sans le badge du collaborateur. Ce système est plus rapide qu'un système entièrement décentralisé car seule une fraction de la quantité de données (une fraction du modèle) doit être échangée par l'interface sans fil. Mais il possède aussi une autre caractéristique: il est impossible de lire les données biométriques utilisables à partir de la carte RFID. Le système biométrique d'accès répond donc entièrement aux exigences de la protection des données.

Outre le contrôle d'accès, le nouveau badge peut être utilisé pour établir la connexion informatique (login) et cela selon le principe de l'authentification unique (single sign on, SSO). Un seul identifiant est donc nécessaire pour toutes les applications informatiques protégées par un mot de passe. Pour le SSO, le modèle d'empreinte digitale crypté dans sa totalité est stocké sur le badge qui est aussi utilisé pour le contrôle d'accès; mais il n'y a aucun stockage centralisé de données biométriques. Le badge peut être introduit à chaque terminal de travail et la connexion peut être établie sans que des données biométriques ne soient transmises sans fil. Le SSO répond ainsi aux exigences posées par la protection des données.

Grâce à l'architecture de ce système, l'entreprise est en mesure de tirer parti des avantages d'un système de reconnaissance biométrique tout en respectant les droits de la personnalité des collaborateurs, notamment le droit de disposer des informations les concernant.

Nous avons établi à ce sujet un guide qui peut être consulté à l'adresse suivante: www.leprepose.ch, Documentation – Protection des données – Brochures – Guide relatif aux systèmes de reconnaissance biométriques.

1.7.3 Remise de certificats des caisses de pension

Le Département fédéral de l'intérieur tarde à empêcher la pratique illicite de la remise des certificats des caisses de pension par l'intermédiaire de l'employeur.

Dans notre 17e Rapport d'activités 2009/2010, ch. 1.7.8, nous avions déjà abordé la pratique de certaines institutions de prévoyance professionnelle qui remettent les certificats aux employés par l'intermédiaire de leur employeur. Etant donné que nous ne disposons pas nous-mêmes de pouvoir de décision, nous avons demandé au Département fédéral de l'intérieur (DFI) en août 2009 d'empêcher cette pratique à notre avis illicite.

Il ne s'est malheureusement pas passé grand chose depuis: Lorsque nous avons posé la première fois la question de l'état de la procédure en février 2010, il nous a été offert de nous exprimer sur un avis rédigé par l'Office fédéral des assurances sociales (OFAS, autorité de surveillance des institutions de prévoyance) en collaboration avec la caisse de pension dont il est question dans le cas concret. Nous avons saisi cette occasion et avons remis notre prise de position à l'OFAS. Depuis juin 2010, l'échange de courrier est clos. La décision du DFI ne nous était pas encore parvenue à la clôture de la rédaction du présent rapport.

La situation juridique est claire à nos yeux. En outre, de nombreuses personnes concernées par cette pratique doivent, aujourd'hui encore, accepter régulièrement une violation de leurs droits de la personnalité et cela aussi longtemps que l'affaire n'aura pas fait l'objet d'une décision applicable. Il nous est donc difficile de comprendre pourquoi le DFI hésite à se prononcer.

1.7.4 Contrôles dans le cadre de commissions professionnelles paritaires

Les contrôles des livres de paye effectués par les commissions professionnelles paritaires tels qu'ils ont été prévus dans la convention collective de travail (CCT) doivent être effectués selon une procédure réglementée. Les employeurs doivent être informés à temps et de manière transparente sur l'ampleur et le déroulement du contrôle ainsi que sur leurs obligations.

Ces dernières années nous avons dû à plusieurs reprises examiner le problème des contrôles des livres de paye dans le domaine des CCT. Le contrôle des livres de paye par des commissions professionnelles paritaires a pour objectif de vérifier que les parties au contrat respectent les dispositions de protection des salaires. La protection des droits de la personnalité des travailleurs doit cependant être assurée et primer sur les intérêts d'une entreprise à maintenir secrètes ses données salariales. Étant donné que l'intérêt de communiquer les données concernées prévaut, nous avons déclaré qu'il n'était pas nécessaire de demander un consentement explicite des travailleurs et d'intégrer cette nécessité dans la CCT. En faisant ces déclarations, nous sommes cependant toujours partis de l'idée que les contrôles menés par les commissions professionnelles paritaires étaient effectués de manière proportionnée et dans la mesure du possible sur place dans un délai raisonnable.

Entre-temps la réalité de l'automatisation et de la numérisation des comptabilités des salaires a rendu notre hypothèse caduque. Il est plutôt rare de nos jours que des membres des commissions professionnelles paritaires ou des tiers mandatés effectuent ces contrôles. Aujourd'hui, afin d'éviter que ceux-ci soient effectués par des concurrents directs, les contrôles de livres de paye sont faits dans la plupart des cas par des contrôleurs professionnels ou des fiduciaires spécialisées. Ces derniers demandent qu'on leur remette les documents nécessaires au contrôle sous forme électronique. Des logiciels de contrôle permettent d'analyser l'ensemble des données de manière bien plus minutieuse et de générer des résultats qu'il n'était auparavant pas possible d'obtenir dans le temps à disposition. L'appréciation de cas concrets a cependant révélé que ces contrôles de livre de paye effectués de manière électronique par des contrôleurs professionnels en dehors des locaux des entreprises concernées soulèvent des inquiétudes concernant la protection et la sécurité des données, notamment auprès des employeurs. Le tout est accompagné d'une peur latente que ce nouveau type de contrôle puisse divulguer trop d'informations propres à l'entreprise.

Il nous apparaît donc nécessaire de faire en sorte que les contrôles des livres de paye ordonnés par les commissions professionnelles paritaires soient définis de manière

transparente dans un règlement. Les employeurs doivent être informés à temps sur l'ampleur et le déroulement des contrôles, ainsi que sur leurs obligations. Dans les cas où le volume des données demandé permet des possibilités de dépouillement insoupçonnées, il sera éventuellement nécessaire de créer d'autres bases et restrictions sur le plan légal. De fait, les CCT mentionnent aujourd'hui déjà des règlements de contrôle. Nos recherches ont cependant révélé que ces derniers n'existaient que sous une forme rudimentaire. Une des commissions professionnelles paritaires nous a assuré qu'elle avait constitué un groupe de travail chargé d'élaborer un tel règlement de contrôle.

1.7.5 Dossier personnel électronique dans l'administration fédérale

Les demandes se font de plus en plus pressantes dans l'administration fédérale pour que les dossiers personnels soient établis sous forme électronique. Les bases légales faisant actuellement défaut, nous avons dû intervenir à deux reprises.

Les organes de la Confédération ne peuvent traiter les données personnelles particulièrement sensibles et les profils de la personnalité que si ce traitement repose sur une base légale, à savoir une loi fédérale. Un dossier personnel constitue en soi un profil de la personnalité et renferme aussi des données personnelles sensibles. Les dispositions en vigueur ne constituent pas une base légale suffisante pour gérer des dossiers personnels sous forme électronique dans l'administration fédérale. Pour cette raison, nous avons dû intervenir dans deux projets. Le premier concernait un système de gestion des dossiers personnels électroniques au sein du Département fédéral de la défense, de la protection de la population et des sports (DDPS) et le deuxième projet un service de candidature en ligne de l'Office fédéral du personnel (OFPER) qui avait donné lieu à des dossiers électroniques. Il n'existe cependant pas encore pour cela non plus de bases légales suffisantes à la Confédération. Suite à notre intervention, le premier projet a été stoppé et l'introduction du second a été repoussée jusqu'à ce que la révision de la loi sur le personnel de la Confédération entre en vigueur (vraisemblablement le 1er janvier 2012).

1.7.6 Traitement de dossiers du personnel dans les systèmes GEVER

Le traitement de dossiers du personnel dans des systèmes GEVER requiert, conformément aux exigences de protection des données, une base légale dans la loi sur le personnel de la Confédération. Cette base légale sera créée avec la révision des articles correspondants.

Suite à une demande de la Chancellerie fédérale, nous avons procédé à une appréciation de la situation juridique actuelle en matière de protection des données concernant le traitement de dossiers du personnel dans les systèmes GEVER et avons pris position.

La loi sur la protection des données (LPD) stipule que les organes fédéraux ne sont autorisés à traiter des données personnelles sensibles et des profils de la personnalité que si ceci est explicitement prévu par une loi au sens formel. La base légale pour les systèmes de gestion des affaires des autorités fédérales est donnée par l'article 57h de la loi sur l'organisation du gouvernement et de l'administration (LOGA), qui permet à tout organe fédéral de gérer un système d'information et de documentation contenant des données sensibles et des profils de la personnalité dans la mesure où ceux-ci «ressortent de la correspondance ou découlent de la nature de l'affaire».

Étant donné que le traitement de dossiers du personnel ne découle pas «de la nature de l'affaire», l'article 57h ne peut pas faire office de base légale dans le cas d'espèce. C'est plutôt la loi sur le personnel de la Confédération (LPers) qui, en complément à la LPD, règle le traitement de dossiers du personnel par les employeurs de la Confédération.

La réglementation actuelle de l'article 27 LPers ne suffit cependant pas à justifier une gestion des dossiers du personnel sous forme électronique. Ceci a été reconnu par le Conseil fédéral qui a, par décision du 1er septembre 2010 relatif au programme de consolidation 12/13, adopté la révision de l'article 27 a-c LPers. C'est cet article qui est censé créer les bases légales nécessaires pour une tenue de dossiers électroniques de demandeurs d'emploi et d'employés. Ceci permettra de prendre en compte le besoin croissant d'utiliser des systèmes de gestion automatisés. Un tel système doit en outre être fermé dans la mesure où les dossiers du personnel traités contiennent des données de santé; il ne doit donc pas être relié à un autre système de traitement de données. Il s'agit là d'une exigence stipulée dans l'ordonnance concernant la protection des données personnelles dans l'administration fédérale.

1.7.7 Contrôle du système d'information du personnel de la Confédération: État actuel

Le règlement de traitement du système informatisé de gestion de données relatives au personnel de la Confédération (BV PLUS) n'est pas encore conforme aux exigences et doit donc être adapté. Certains aspects doivent encore être améliorés ou documentés, en particulier le téléchargement de données, la journalisation et les procédés de contrôle.

Lors de notre contrôle du système central informatisé de gestion du personnel de la Confédération (BV PLUS), nous avons constaté de manière générale que la documentation dans le domaine de la protection et de la sécurité des données n'était pas très volumineuse. Ainsi, le règlement de traitement a été rédigé il y plusieurs années sans être vraiment mis à jour depuis. Nous avons donc attiré l'attention des personnes responsables sur nos explications relatives à l'élaboration d'un tel règlement (voir sur notre site web www.leprepose.ch, sous Documentation – Protection des données – Brochures – Mesures techniques et organisationnelles).

En outre, nous avons aussi constaté qu'au début de notre contrôle, l'expert de sécurité de l'information du système progiciel SAP, sur la base duquel BV PLUS est exploité, n'était pas présent. À notre avis, il est indispensable qu'une personne compétente soit disponible lorsqu'on exploite un système si sensible pour l'ensemble de la Confédération. Ce professionnel devrait agir comme interlocuteur aussi bien pour les fournisseurs de prestations (tels que les centres de calcul) que pour les bénéficiaires des prestations (tels que les services du personnel) et être en mesure d'assumer ses tâches de manière aussi indépendante que possible.

Tous les utilisateurs, à l'exception de ceux d'une unité organisationnelle relativement importante, ont utilisé des cartes à puce de la classe B pour s'authentifier. Nous avons attiré l'attention sur le fait qu'il serait souhaitable, vu la nature sensible des données traitées dans ce système, que tout le monde se serve de cartes à puce pour s'authentifier. Notre recommandation a par la suite été suivie.

Le système SAP ou BV PLUS permet de télécharger des données sur l'ordinateur à la place de travail ou depuis celui-ci sur le système informatique SAP. De tels téléchargements permettent de contourner les restrictions d'accès du système SAP central. Nous n'avons pas pu trouver d'indications utiles dans le règlement de traitement sur ces opérations. Du point de vue de la protection des données, il doit être possible de savoir qui est autorisé, pour quelle raison (à quelle fin) à effectuer ces téléchargements. Le règlement doit également indiquer quelles sont les données requises pour ces téléchargements et comment les données transmises sont ensuite traitées sur les ordinateurs. Si la procédure est la même pour toutes les unités organisationnelles, il suffit

qu'elle soit documentée une seule fois. Toutefois, si il existe des divergences au sein de l'administration fédérale, les procédures doivent être documentées en conséquence. Lors de notre contrôle, on nous a signalé qu'il n'existait pas de moyen technique judicieux pour la journalisation des téléchargements. Pourtant, le guide de protection des données pour SAP ERP 6.0 publié par le groupe de travail «Protection des données» de DSAG, le groupe allemand d'utilisateurs de SAP, décrit une telle journalisation moyennant les «Security Audit Logs».

On nous a également informés qu'il n'existait pas de moyens techniques appropriés pour journaliser des requêtes BW de nature sensible. Pourtant, le guide susmentionné explique clairement (au point 4.2.1.9.6) comment effectuer ad hoc de telles journalisations de requêtes. Sur la base des documents qu'on nous a remis et des points contestés, nous avons conclu qu'il était entre autres nécessaire d'agir au niveau de la journalisation. C'est pourquoi nous avons demandé aux responsables de mettre sur pied un concept de journalisation qui réponde aux exigences de la protection des données. Cette dernière doit non seulement tenir compte des besoins du fournisseur des prestations, mais également de ceux des bénéficiaires des prestations.

Comme procédure de contrôle en cours d'exploitation, il a été décidé que le fournisseur de prestations analyse ponctuellement les journaux du système. Les contrôles doivent cependant aussi être effectués en cours d'exploitation par les maîtres de fichier. Les procédures de contrôles correspondantes doivent être documentées.

Les responsables nous ont communiqué que l'application des points encore en suspens durera jusqu'à fin 2011.

1.8 Économie et commerce

1.8.1 La protection des données et l'utilisation de compteurs électriques intelligents

La nouvelle loi sur l'approvisionnement en électricité prévoit une libéralisation par étapes du marché de l'électricité à partir du 1er janvier 2008. Ceci nécessite une nouvelle méthode de saisie des consommations. Des compteurs numériques permettent d'enregistrer et de transmettre en ligne un volume important de données, ce qui permet d'une part de montrer aux consommateurs les potentiels d'économie d'énergie, mais présente d'autre part également des risques pour la sphère privée.

Avant la mise en œuvre d'un projet pilote avec 480 compteurs numériques, appelés «compteurs intelligents», un fournisseur d'énergie nous a contactés pour que nous donnions notre avis sur l'aspect protection des données de la conception du projet. Nous avons conclu qu'il était nécessaire d'informer de manière détaillée les ménages concernés pour le cas où – dans le cadre du projet pilote – il serait prévu d'enregistrer le profil de charge complet (consommation d'énergie pour une période donnée) pour le transmettre au fournisseur d'énergie qui l'enregistrera pour l'analyser. Les personnes concernées peuvent demander à ce que seule leur consommation d'électricité aux tarifs «heures pleines» et «heures creuses» soit relevée, l'enregistrement du profil de charge par intervalle de 15 minutes n'étant pas nécessaire pour la facturation.

Indépendamment du projet pilote, nous avons – en vue de la deuxième étape de l'ouverture du marché de l'électricité – également évalué les risques en matière de protection des données liés à l'utilisation de tels compteurs intelligents. Les compteurs intelligents permettent, selon leur configuration, d'enregistrer de manière plus ou moins détaillée des profils de charge (soit les valeurs de la consommation par intervalle de saisie) d'un ménage et aussi de relever ces données à distance. Pour un intervalle de saisie de 15 minutes, ceci correspond à 35000 points de mesure par an. Un tel profil de consommation d'énergie fournit aux consommateurs d'électricité des informations précieuses sur leur consommation d'énergie ainsi que sur les potentiels d'économies, mais aussi des informations sur leurs activités professionnelles, leurs processus de production, leurs activités personnelles, l'organisation de leurs journées, leurs absences maladie, etc. Le profil de consommation d'énergie constitue ainsi un profil de la personnalité qui ne peut être relevé de manière générale. À notre avis, ni la planification des réseaux ni la facturation ne requièrent impérativement que des informations d'un tel degré de détail soient communiquées de manière automatique.

Des explications sur l'utilisation des compteurs intelligents dans le cadre de Smart Grid se trouve à l'annexe 4.1.1 et sur notre site www.leprepose.ch sous Thèmes – Protection des données – Autres thèmes.

1.8.2 Communication de données à l'étranger dans le cadre de l'externalisation (outsourcing) du traitement de données

En cette époque de mondialisation, la communication de données à l'étranger dans le cadre d'une externalisation est de plus en plus fréquente, particulièrement dans le cas des groupes internationaux de sociétés. En outre, conséquence de la division du travail, il n'est pas rare aujourd'hui que le traitement des données soit confié à un sous-mandataire. La question se pose donc de savoir quelles sont les conditions en matière de protection des données qui doivent être remplies pour que la communication de données à un mandataire et à un sous-mandataire à l'étranger soit licite.

La loi sur la protection des données prévoit que le traitement de données personnelles peut contractuellement être confié à un tiers, à savoir un mandataire. Toutefois, selon la loi, ces traitements sont limités à ceux que le mandant serait lui-même en droit d'effectuer. Il découle de cette obligation qu'un mandataire qui désire confier le traitement de données à un sous-mandataire doit conclure avec celui-ci un contrat et que le sous-mandataire n'est à son tour en droit d'effectuer que les traitements que le mandant ou le mandataire seraient eux-mêmes en droit d'effectuer. Ces exigences légales valent indépendamment du fait de savoir si le traitement des données est effectué par un (sous-)mandataire en Suisse ou l'étranger. Si le (sous-)mandataire se trouve à l'étranger, les dispositions de l'art. 6 LPD sont en outre applicables.

Nous avons publié des documents concernant la communication de données à l'étranger dans le cadre d'une externalisation. On y trouve les principaux cas d'externalisation ainsi que les directives à observer en matière de protection des données (cf. www.leprepose.ch, sous la rubrique Thèmes – Transmission à l'étranger).

Par ailleurs, nous avons remanié le contrat-type pour l'externalisation du traitement de données à l'étranger («Swiss Transborder Data Flow Agreement») et l'avons complété par des dispositions concernant le traitement de données par un sous-mandataire (uniquement en anglais). Une telle transmission du traitement de données n'est

désormais possible qu'avec le consentement préalable écrit du mandant; en outre, le mandataire est tenu de conclure avec le sous-mandataire un contrat écrit dans lequel ce dernier s'engage à respecter les mêmes normes de protection des données que son mandant (direct). Le contrat-type peut être téléchargé sur notre site (www. leprepose.ch, sous la rubrique Thèmes – Transmission à l'étranger).

Mentionnons enfin que la Commission de l'Union européenne s'est également penchée sur le sujet et a récemment modifié ses «Clauses Contractuelles Types pour le transfert de données à caractère personnel vers des sous-traitants», qui sont entrées en vigueur le 15 mai 2010.

1.8.3 Utilisation de données de clients bloquées à des fins de publicité

Un citoyen a attiré notre attention sur le cas d'une banque suisse qui envoie, en même temps que les extraits de compte périodiques, du matériel d'information alors que le client a expressément interdit l'utilisation de son adresse à des fins de publicité. Nous avons donc examiné les mesures techniques et organisationnelles de la banque relatives au blocage des adresses. Nous avons constaté que la banque n'envoie pas de publicité si l'adresse est bloquée, mais uniquement le matériel d'information conformément au devoir de diligence relevant du droit bancaire. L'envoi de cette documentation est donc justifié.

L'adresse d'un client peut être utilisée à des fins de publicité tant que celui-ci ne l'a pas bloquée. Mais en cas de blocage de l'adresse, l'entreprise doit garantir aux niveaux organisationnel et technique que celui-ci est effectivement respecté. Les lettres d'information qui contiennent des renseignements importants pour les clients de la banque ou qui leur signalent, par exemple, une modification des conditions contractuelles ou des informations de base sur les placements effectués par leur clientèle doivent cependant être différenciées du matériel publicitaire. La banque dispose dans ce cas d'un motif justificatif pour utiliser les données clients même contre la volonté des personnes concernées. Mais cela uniquement dans la mesure où l'accomplissement de son devoir de diligence l'exige.

Comme nous l'avons constaté, la banque fait une distinction claire entre les envois relevant purement de la publicité et les lettres d'information qu'elle a l'obligation légale d'envoyer. Dans le premier cas, elle donne la possibilité d'une option de retrait (opt-out): si un client ne souhaite pas d'envoi publicitaire, il doit en informer la banque. Dans son fichier clients, la banque peut supprimer la possibilité d'envoyer de la publicité, d'une manière générale ou par thème, pour chaque client qui le demande. Ainsi,

les clients reçoivent des envois publicitaires que dans la mesure où ils le souhaitent. Les envois effectués dans le cadre du devoir d'information ne peuvent par contre pas être bloqués.

Ainsi, la banque utilise ses données clients à des fins de publicité en conformité avec ses obligations en matière de protection des données de sorte que nous n'avons à cet égard aucune critique à émettre.

1.8.4 Traitement de données dans le commerce d'adresses

Des sociétés spécialisées dans le commerce d'adresses collectent des données diverses sur les consommateurs afin de les vendre à des tiers. Un tel traitement de données est admis pour autant qu'il respecte les règles prescrites par la législation sur la protection des données, notamment les principes de finalité et de transparence. Les personnes concernées doivent avoir la possibilité de s'opposer à ce que leurs informations personnelles soient utilisées à des fins commerciales et d'accéder à toutes les données qui les concernent.

Les sociétés commerciales, associations, journaux ou revues cherchent à conquérir de nouveaux clients, de nouveaux donateurs ou de nouveaux abonnés et cherchent à mieux connaître leur clientèle afin de la fidéliser ou de tirer plus de profit des clients disposant du plus fort potentiel. Dans ce but, il est utile – pour une société de vente par correspondance par exemple – de disposer d'un maximum de données sur sa clientèle réelle ou potentielle. En effet, plus une société connaît sa clientèle, plus elle sera en mesure de lui proposer des produits ou des services correspondant à ses besoins et susceptibles de l'intéresser et mieux elle pourra vendre ses produits ou ses prestations.

Certaines sociétés se sont spécialisées dans le traitement d'adresses et de fichiers clients en collectant de nombreuses informations sur les consommateurs. Elles proposent à toute personne ou société intéressée de mettre à disposition leurs fichiers, en lui vendant ou en lui louant les adresses d'un groupe cible (vente d'adresses) ou en enrichissant les fichiers clients de la personne/société par des informations supplémentaires (enrichissement de données).

En plus des adresses, qui sont puisées dans les annuaires téléphoniques ou encore fournies par des tiers, les sociétés spécialisées dans la vente d'adresses disposent de nombreuses autres informations sur les individus ou les sociétés qu'elles collectent ici et là (concours, questionnaire sur les habitudes de consommation, etc.) ou qui sont fournies par d'autres sociétés partenaires. Elles les compilent avec d'autres données – p.ex. le coût de construction de l'immeuble à une adresse donnée ou encore des données statistiques – avant de mettre leurs fichiers ciblés à disposition de leurs clients.

À partir de divers critères (tels que le sexe, l'âge, la région ou encore la profession) ou encore d'indications sur les habitudes de consommation (telles que le pouvoir d'achat, la propension à acheter par correspondance ou les loisirs), une société de vente par correspondance qui propose une ligne de vêtements de luxe pour bébés peut ainsi acheter les adresses et numéros de téléphone de son public cible, à savoir par exemple les femmes de 30 à 40 ans, vivant dans une région donnée, avec des enfants en bas âge, disposant d'un revenu élevé et achetant facilement par correspondance. Cette même société de vente par correspondance peut également compléter les profils de sa clientèle en complétant les informations dont elle dispose déjà par de nouvelles indications, telles que la date de naissance ou le nombre d'enfants, ou encore le numéro de téléphone, afin de proposer des offres adaptées aux intérêts de ses clients – selon leur profil – et de diversifier les canaux de marketing.

Il va de soi que la collecte de données sur des personnes déterminées ou l'attribution de profils tombe dans le champ d'application de la loi fédérale sur la protection des données. Celle-ci n'interdit pas la mise à disposition de fichiers, mais définit un certain nombre de règles à respecter.

Nous sommes en train d'examiner si, dans la pratique, les traitements des données effectués dans le domaine du commerce d'adresses sont bien conformes aux prescriptions de la LPD, en particulier au principe de finalité et de transparence (notamment quant à l'origine des données collectées). De même, nous examinons si les personnes qui exercent leur droit d'accès auprès de ces sociétés spécialisées reçoivent la totalité des informations contenues dans les fichiers et si leur droit d'opposition est bien respecté.

1.8.5 Contrôle de l'âge aux distributeurs de cigarettes

Sur certains distributeurs de cigarettes en Suisse, le système actuel à jetons pour la contrôle de la limite d'âge est remplacé par un lecteur de cartes. Ce système, tel qu'il nous a été présenté, ne pose aucun problème du point de vue de la protection des données.

La société British American Tobacco nous a présenté son nouveau système de lecture de carte pour ses distributeurs de cigarettes. Il est mis en service dans divers endroits et remplace le système actuel à jetons. Avec ce dernier, le contrôle de l'âge était effectué par le restaurateur ou le personnel du local dans lequel se trouvait le distributeur. Le nouveau système par contre peut lire la carte d'identité ou le permis de conduire. Le contrôle de l'âge est effectué sur la base de la date de naissance, du type

de document et de son authenticité. Le lecteur de cartes reconnaît si l'acheteur (potentiel) a atteint l'âge minimal prescrit, dans quel cas il permet d'effectuer l'achat sur le distributeur de cigarettes.

Le système de lecture de cartes n'est pas en mesure d'éviter les abus, p. ex. l'utilisation d'une pièce d'identité appartenant à une autre personne. Nous considérons cependant que ce système ne pose aucun problème du point de vue de la protection des données, puisque toutes les données ne sont enregistrées que de manière temporaire et sont ensuite irrévocablement détruites et que ces données ne sont pas exploitées.

1.8.6 Collecte de données pour une carte à prépaiement

Les informations concernant le revenu ne sont requises que pour les cartes de crédit. Le fait d'exiger ces données pour une carte à prépaiement est disproportionné et n'est pas conforme à la loi fédérale sur la protection des données. Donnant suite à notre requête, un émetteur de cartes a adapté ses formulaires en conséquence.

Suite à une information d'une personne concernée, nous avons examiné le formulaire de demande d'un abonnement demi-tarif combiné avec une carte de crédit ou une carte à prépaiement. La personne souhaitant obtenir une telle carte devait remplir un formulaire dans lequel il devait fournir des informations personnelles et professionnelles. Il était en particulier précisé que toutes ces données – notamment celles sur la source et le montant de ses revenus – étaient impératives et que faute d'indications, la demande ne serait pas traitée.

Conformément à la loi fédérale sur le crédit à la consommation, le prêteur (respectivement l'émetteur d'une carte de crédit) a l'obligation de vérifier si le consommateur a bien la capacité de contracter un crédit. La vérification des sources de revenus a pour but d'empêcher un éventuel surendettement occasionné par un tel contrat. Cette obligation légale ne vise cependant que les contrats de crédit à la consommation.

Dans le cas d'une carte à prépaiement, il n'est pas nécessaire d'obtenir des informations sur le revenu. La carte à prépaiement permet en effet de disposer du montant versé préalablement sur la carte sans aucun risque de surendettement. Par conséquent, le fait d'exiger également des informations sur le revenu n'est pas conforme aux principes de finalité et de proportionnalité et est, en l'absence de motif justificatif, contraire à la loi fédérale sur la protection des données.

À notre demande, l'émetteur de cartes concerné a accepté d'adapter ses formulaires en précisant que les données concernant les revenus n'étaient requises que pour une demande de carte de crédit.

1.9 Finances

1.9.1 Manque d'uniformité dans la communication des extraits de registres des poursuites

Les offices cantonaux des poursuites n'ont pas une pratique uniforme en matière de communication des extraits des registres des poursuites. Certains offices ne communiquent que des données remontant à deux ans, d'autres à cinq ans. Quelques-uns communiquent même des données qu'ils ne devraient selon la loi plus du tout divulguer.

Dans le cadre de nos recherches sur le traitement de données d'ordre économique et de données relatives à la solvabilité par des agences d'évaluation du crédit et des agences de renseignement économique, nous avons fait établir une expertise externe qui était consacrée au caractère proportionnel de ces traitements (cf. notre 17e rapport d'activités 2009/2010, ch. 1.9.5). L'expert mandaté a constaté à cette occasion que la communication des extraits des registres par les offices cantonaux des poursuites, conformément à l'art. 8a de la loi fédérale sur la poursuite pour dettes et la faillite (LP), ne correspondait pas à une pratique uniforme, tant du point de vue des délais que du contenu. Certains offices ne communiquent que des informations concernant les deux années précédentes, d'autres par contre les cinq années précédentes. En outre, certains offices communiquent même des données concernant des poursuites qu'ils ne devraient manifestement pas (plus) communiquer conformément à la LP. Du fait de leur portée économique, ces données doivent être classées comme étant délicates. Dans certains cas, ces pratiques peuvent avoir des répercussions dommageables pour les personnes demandant un crédit parce qu'elles se heurtent à un refus éventuellement injustifié ou qu'on ne leur accorde un crédit qu'à des conditions défavorables.

Etant donné que la loi sur la protection des données n'est pas applicable aux registres publics relatifs à des rapports de droit privé, dont font partie les registres des poursuites, nous avons contacté l'Office fédéral de la justice (OFJ) qui exerce la haute surveillance sur les offices des poursuites. Nous lui avons exposé la situation et les problèmes pouvant survenir dans le contexte de ces pratiques inégales. L'OFJ est au courant de cette hétérogénéité dans la communication des données figurant aux registres des poursuites.

1.9.2 Traitement de données d'ordre économique et de données relatives à la solvabilité par des sociétés de renseignement

Le traitement de données relatives à la solvabilité par des agences d'évaluation du crédit et des agences de renseignement économique touche deux thèmes principaux: d'une part la correction et l'effacement de données fausses, entreprise qui s'avère dans la pratique longue et fastidieuse; d'autre part, les possibilités qu'offre actuellement la technique en matière de collecte et de mise en relation de données permettent la création de profils de la personnalité.

Le traitement de données d'ordre économique et de données relatives à la solvabilité par des agences d'évaluation du crédit et des agences de renseignement économique demeure un thème qui suscite beaucoup de questions de la part des citoyens. Dans la plupart des cas, il s'agit de l'effacement et de la correction de données erronées, du contenu et du volume licite des données traitées ainsi que du droit d'accès.

Force est de constater que le traitement de données relatives à la solvabilité est encore source d'erreurs: Deux individus sont confondus ou alors une personne se voit attribuer un mauvais «score» en matière de crédit, c'est-à-dire une solvabilité négative. Selon les circonstances, cela peut avoir pour cette personne des répercussions sévères, si ce n'est extrêmement dommageables en matière de crédit. Dans la pratique, la correction ou l'effacement de données erronées s'avère une entreprise longue et fastidieuse, liée à de nombreuses démarches, car très souvent ces données doivent être corrigées dans plusieurs fichiers auprès de différentes agences et il peut arriver qu'une personne ne sache même pas où de fausses données sont stockées sur elle.

Nous observons par ailleurs la tendance d'agences d'évaluation du crédit et de renseignement économique de rassembler – grâce aux possibilités qu'offre aujourd'hui la technique – des données de plus en plus nombreuses et détaillées sur des personnes et de les relier ensuite les unes aux autres. Ainsi, il est courant aujourd'hui que des données concernant la solvabilité soient complétées par des informations sociodémographiques et géographiques et on peut se demander si elles ne servent pas de base à l'établissement de profils de la personnalité.

Face à cette évolution, nous allons poursuivre nos investigations auprès des agences d'évaluation du crédit et des agences de renseignement économique dans le cadre de notre activité de surveillance.

1.9.3 Accord de double imposition

La loi sur la protection des données doit également être respectée dans l'entraide administrative transfrontière en matière fiscale. Les nouvelles conventions internationales de double imposition, adaptées au standard de l'OCDE, excluent l'échange automatique d'informations ainsi que les «fishing expeditions». En outre, l'entraide administrative n'est pas accordée dans le cas des données acquises illégalement.

Depuis que le Conseil fédéral a décidé, le 13 mars 2009, de développer l'entraide administrative internationale en matière fiscale et d'adopter le standard de l'OCDE (notamment l'échange d'informations), de nombreuses conventions de double imposition (CDI) ont été révisées ou nouvellement conclues. Etant donné que la loi sur la protection des données doit aussi être respectée dans l'entraide administrative internationale, nous avons reçu, dans chaque cas lors de la consultation des offices, la possibilité de nous exprimer sur ces conventions.

Du point de vue de la protection des données, les CDI concernées sont toutes celles qui ont été adaptées au standard de l'OCDE, à savoir dans lesquelles la réglementation relative à l'échange d'informations en matière fiscale (art. 26 du modèle de Convention de l'OCDE) a été reprise. Cette disposition établit entre autres que les informations fiscales ne peuvent être échangées que si l'État requérant identifie clairement, dans une demande d'entraide administrative, le contribuable concerné ainsi que le service ou la personne (par ex. une banque) supposé être en possession des données souhaitées. En outre, l'État requérant doit indiquer les informations dont il a besoin, pour quelles périodes fiscales et dans quels buts de nature fiscale. Il en découle que l'échange d'informations se limite à des demandes concrètes concernant un cas d'espèce et que les «fishing expeditions», à savoir les requêtes présentées sans objet d'investigation précis dans l'espoir d'obtenir les informations fiscalement déterminantes, sont expressément exclues. Enfin, les CDI prévoient expressément que l'entraide administrative en matière fiscale n'est pas accordée lorsque la demande d'entraide se fonde sur des données obtenues illégalement.

Étant donné la situation, nous estimons que l'échange d'informations avec l'étranger en matière fiscale est conforme avec la loi sur la protection des données.

1.10 International

1.10.1 Coopération internationale

La dimension internationale des questions liées à la protection des données ne cesse de croître. Elle nécessite une intensification de la coopération entre les autorités de protection des données en Europe et dans le monde. Elle renforce également la volonté de parvenir à un instrument juridique universel contraignant. 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

Le comité des Ministres du Conseil de l'Europe a adopté le 23 novembre 2010 la recommandation R (2010) 13 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage (www.coe.int). Cette recommandation préparée par le comité consultatif (T-PD) de la Convention 108 (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) constitue le premier texte juridique énonçant des normes minimales de protection des données dans le domaine du profilage des individus. Les États membres du Conseil de l'Europe sont ainsi invités à mettre en œuvre les principes de la recommandation par le biais de la législation nationale et de l'autorégulation. Le profilage consiste à observer le comportement des individus, à collecter et à exploiter leurs données personnelles. Cette technique est de plus en plus pratiquée dans de nombreux secteurs d'activités, en particulier ceux liés à la société de l'information et à Internet. La recommandation ne tend pas à interdire le recours au profilage lorsque la finalité du traitement est légitime, mais à donner un cadre réglementaire cohérent et équilibré à ces pratiques et techniques. Elle énonce les conditions nécessaires à prévenir des violations de la protection des données et de la vie privée, notamment le risque de discrimination. Face à la complexité, voire à l'opacité de cette technique de traitement des données, il est important de garantir la transparence en renforçant les exigences liées à l'information des personnes concernées et en octroyant à ces dernières des droits supplémentaires afin qu'elles aient la pleine maîtrise sur leurs données et qu'elles puissent agir en connaissance de cause. Il est également important d'ancrer au niveau légal l'obligation de recourir à des technologies conformes à la protection des données.

Le T-PD a renouvelé son bureau et élu à sa présidence le représentant suisse en la personne du préposé fédéral suppléant. Il a en outre entamé ses travaux en vue de la modernisation des instruments juridiques du Conseil de l'Europe régissant la protection des données et notamment la convention 108 et son protocole additionnel, la recommandation R (89) 2 sur la protection des données à caractère personnel utilisées à des fins d'emploi et la recommandation R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police.

Ces travaux devraient déboucher sur une modification de la convention, sous forme d'amendement ou de protocole additionnel. En affirmant le droit à la maîtrise sur les données, le droit à la dignité humaine et à la non-discrimination lors du traitement de données personnelles, la place de l'individu en tant que sujet des données qui font l'objet de traitement s'en verrait renforcée. Les principes de base de la protection des données devraient être complétés ou précisés (notamment par le principe de minimisation des données, le principe du développement conforme à la protection des données dès la conception de systèmes «Privacy by Design», de services ou de produits, le principe de responsabilité «renforcée»). Une obligation d'informer lors de failles de sécurité pourrait ainsi être introduite. En outre, les droits des personnes concernées devraient être renforcés, notamment en introduisant explicitement le droit à l'information, le droit à l'oubli ou le droit à ne pas être soumis à une décision automatisée. Une attention particulière devrait être apportée à la mise en œuvre et aux moyens pour les personnes concernées de faire valoir leurs droits. Le caractère général, simple et technologiquement neutre de la convention devra être préservé. De même, l'objectif de permettre à des États tiers non membres du Conseil de l'Europe d'adhérer à l'instrument devra être pris en compte.

Ce travail de modernisation a reçu l'aval du comité des Ministres le 10 mars 2010 et fait l'objet d'une résolution sur la protection des données et la vie privée au troisième millénaire adoptée à Istanbul, le 26 novembre 2010 lors de la 30e conférence du Conseil de l'Europe des Ministres de la justice (www.coe.int). Nous avons présenté le projet de modernisation de la Convention lors d'une conférence organisée conjointement par le Conseil de l'Europe et la Commission européenne le 28 janvier 2011 à l'occasion du 30e anniversaire de la Convention 108 et de la 5e journée européenne de la protection des données.

Enfin, le Conseil de l'Europe poursuit ses efforts en vue de l'adhésion d'États tiers à la Convention 108 et à son protocole additionnel et pourrait accueillir une première adhésion en 2011.

Conférence européenne des commissaires à la protection des données

La conférence européenne de printemps des commissaires à la protection des données s'est tenue à Prague du 29 au 30 avril 2010 et a été organisée par l'Office tchèque de la protection des données. Intitulée «Penser le passé, en pensant à l'avenir», la conférence a en particulier abordé des questions liées à l'Internet des choses et à la protection des données des enfants, et examiné notamment plusieurs campagnes de sensibilisation menés par différentes autorités en Europe. Elle s'est également penchée sur le futur du cadre juridique de la protection des données au sein de l'Union européenne et du Conseil de l'Europe. La conférence a adopté quatre résolutions, portant sur l'avenir de la protection des données, sur le projet d'accord entre l'Union européenne et les États-Unis relatif à des normes de protection des données dans le domaine de la police et de la coopération judiciaire en matière pénale, sur les scanners corporels et sur la protection des enfants, notamment par la mise en place d'actions conjuguées de sensibilisation et d'éducation (voir sur notre site www.leprepose.ch, sous Thèmes – Protection des données – Coopération internationale)

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 positions. Nous avons participé aux différentes réunions de juin, octobre et décembre 2010. Le groupe de travail a en particulier établi une méthodologie commune d'évaluation des risques préalablement aux inspections de données afin de renforcer l'efficacité de la surveillance.

Le groupe de travail a rendu un avis sur la création d'un cadre européen pour la communication des données PNR aux pays tiers et pour l'utilisation des données PNR à des fins répressives. Un autre avis relève l'insuffisance de la protection des données telle que prévue pour l'accord-cadre entre l'UE et les États-Unis relatif à l'échange des données à caractère personnel. De plus, le groupe de travail a adopté plusieurs résolutions, notamment portant sur la cybercriminalité, sur les scanners corporels utilisés à des fins de contrôle dans les aéroports ainsi que sur les accords bilatéraux en matière répressive conclus avec les États tiers. Il a aussi pris position sur la révision du cadre juridique de protection des données de l'UE instaurée par le Traité de Lisbonne. Il examine actuellement les diverses formes de surveillance coordonnée envisageables ainsi que l'avenir du groupe de travail.

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 les méthodes de contrôle utilisées par les autorités de protection des données en fonction de leurs compétences légales respectives. En septembre 2010, le groupe de travail, constitué de représentants de 25 autorités nationales de protection des données, a examiné les différentes étapes indispensables au bon déroulement d'une procédure de contrôle ou du traitement d'une plainte.

Quatre étapes ont ainsi pu être mises en évidence: Le premier contact avec l'organe contrôlé, l'évaluation du cas et la préparation du contrôle, la réalisation du contrôle et finalement l'exécution des mesures ou des sanctions émises.

S'agissant du premier contact avec l'organe contrôlé, il est ressorti des travaux du groupe de travail et des échanges d'expériences entre les participants que cette étape est essentielle pour la réussite du contrôle envisagé, à tout le moins pour la mise en place des meilleures conditions possibles à sa réalisation. Pour bon nombre d'autorités, la législation prévoit des contrôles sous forme d'éclaircissements des faits et permet d'exiger la production de pièces, de demander des renseignements et la présentation des traitements. L'éclaircissement des faits implique une collaboration de l'organe contrôlé. Il est donc primordial que le premier contact se fasse dans de bonnes conditions et qu'une information claire et complète soit donnée à l'organe contrôlé sur le cadre et l'étendue du contrôle qui va avoir lieu, ainsi que sur les bases légales y relatives.

La deuxième étape de la procédure de contrôle ou du traitement d'une plainte est l'évaluation du cas et la préparation du contrôle. Lorsque ce dernier est d'une certaine étendue, il est nécessaire d'élaborer une esquisse de projet fixant les limites du contrôle, les questions à poser, les acteurs concernés ainsi que la planification prévue. L'esquisse de projet permet de délimiter l'ampleur du contrôle envisagé tant sur le plan matériel que temporel. Les expériences des différents participants ont mis en lumière que cette phase préparatoire peut extrêmement varier dans sa durée selon les contrôles mis en place. Il a également été relevé que certaines autorités fixent un plan des contrôles à effectuer durant l'année en se concentrant sur des domaines précis ou en tenant compte de cas problématiques annoncés alors que d'autres autorités organisent leurs activités de contrôle avant tout en fonction des plaintes reçues. Tous les participants du groupe de travail ont insisté sur la difficulté de fixer des priorités dans les activités de contrôle compte tenu des ressources limitées à disposition.

La troisième étape est la réalisation du contrôle. Celle-ci comprend en principe l'analyse de la documentation fournie par l'organe contrôlé ainsi que la visite sur place, et prend fin avec la rédaction d'un rapport de contrôle. Il est ressorti des discussions du groupe de travail que la visite sur place est un élément fondamental dans le processus d'un contrôle et que très peu d'activités de surveillance peuvent être réalisées sur de simples échanges de courriers ou de documentations. Les représentants d'autres autorités nationales ont, comme nous, constaté que c'est en se rendant sur place, en examinant les pièces sur le lieu du traitement et en posant les questions sur la base d'une vision locale que l'autorité de contrôle peut effectuer de manière approfondie sa tâche et dans de très nombreux cas découvrir des pratiques problématiques dans les traitements de données qui n'auraient pas pu être détectées sur la seule base de la documentation livrée par l'organe contrôlé.

La quatrième et dernière étape est l'exécution des mesures ou des sanctions émises: il s'agit de la mise en œuvre des mesures prévues dans le rapport final de contrôle. Nous établissons ainsi des recommandations à l'issue de nos rapports si des manquements ont été constatés ou si des prescriptions sur la protection des données ont été violées. Lors de la discussion, on a pu constater 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. Il sera nécessaire de prendre en compte cette réalité et d'envisager de telles possibilités dans le cadre d'une nouvelle révision de la loi fédérale sur la protection des données, éventuellement suite à l'évaluation en cours de cette loi (voir chiffre 3.1).

Groupe de coordination de la surveillance Eurodac

Le groupe de coordination de la surveillance Eurodac exerce la surveillance des données traitées dans le cadre du système d'information Eurodac en matière d'asile. Il coordonne les activités de surveillance entre les autorités nationales de protection des données et le contrôleur européen à la protection des données ainsi que le suivi législatif. Nous avons participé aux réunions de mars, octobre et décembre 2010.

Le groupe de coordination mène actuellement une inspection conjointe concernant la destruction anticipée de données dans le système Eurodac, c'est-à-dire l'effacement définitif de données avant le délai légal de leur effacement automatique. Nous participons à cette inspection coordonnée en menant un contrôle auprès de l'Office fédéral des migrations.

Quant au suivi législatif, le groupe de coordination a pris position sur la révision des règlements Eurodac et Dublin. Cette refonte a, à ce stade, donné lieu à une résolution du Conseil et du Parlement européen qui élargit l'accès du système Eurodac aux autorités répressives en cas d'infractions graves ou de terrorisme. Il a aussi pris position sur la proposition législative de la Commission qui établit les compétences de la nouvelle agence pour la gestion opérationnelle des systèmes d'information à large échelle dans le domaine de justice, liberté et sécurité (agence IT) concernant Eurodac. Par ailleurs, le groupe de coordination a consulté des représentants de la société civile en matière d'asile afin d'évaluer les problèmes et les meilleures pratiques.

Autorité de contrôle commune Schengen

L'autorité de contrôle commune Schengen (ACC) s'est réunie à quatre reprises en 2010. L'ACC a en particulier préparé des avis sur l'interprétation des dispositions de la convention d'application des accords de Schengen, a poursuivi ses activités de contrôle et planifié de nouvelles inspections. Elle a adopté le rapport de suivi des recommandations émises lors de l'inspection relative aux alertes concernant les signalements d'étrangers aux fins de non admission. L'ACC constate qu'un contrôle de suivi est opportun et qu'il démontre des différences entre États membres dans la prise en compte des recommandations émises. Elle invite les autorités compétentes à demeurer vigilantes et à assurer un contrôle effectif. À notre demande, l'ACC s'est entretenue de la pratique de certaines autorités cantonales de police consistant à systématiquement comparer les fiches d'hôtel avec les signalements du SIS et a convenu de préparer un avis sur l'interprétation de l'article 45 de la convention d'application qui régit l'obligation de s'enregistrer dans les lieux d'hébergement et la mise à disposition des fiches de déclaration aux autorités compétentes. Dans ses premières conclusions, l'ACC est d'avis qu'une vérification automatique et systématique de tous les signalements du SIS avec les fiches de déclaration n'est pas conforme à la convention d'application. L'ACC mènera en 2011 une 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. Elle conduira également une inspection concernant les alertes relatives aux personnes recherchées pour l'arrestation aux fins d'extradition.

Conférence internationale des commissaires à la protection des données

La 32e conférence internationale des commissaires à la protection des données et à la vie privée s'est tenue à Jérusalem du 26 au 29 octobre 2010 à l'invitation de l'autorité israélienne de la protection des données (www.privacyconference2010.org). Cette conférence a rassemblé quelque 600 participants issus des autorités de protection des

données, des gouvernements, du secteur privé, de monde académique et de la société civile. Placée sous le thème «Vie privée: générations», la conférence a débattu des changements de comportement des individus influencés par le développement continu des technologies de l'information et des communications indépendamment des frontières. Elle a abordé également les risques que ces technologies génèrent pour le respect des droits et des libertés fondamentales, notamment le droit à la vie privée.

Les participants ont ainsi traité de nombreux sujets liés à l'Internet des objets, aux réseaux sociaux, aux développements du cadre juridique de la protection des données, au rôle des différents acteurs et à leurs responsabilités et à leurs obligations en matière de protection des données, aux technologies et aux instruments permettant le respect de la vie privée en ligne. Des questions sensibles touchant au droit applicable, au consentement, au droit à l'oubli ou à l'accès des gouvernements aux données personnelles du secteur privé ont également été discutées. La conférence a démontré que si les comportements changent, les préoccupations de protection de la vie privée demeurent, quelles que soient les générations. La technologie doit, plus que jamais, être au service des individus, en particulier en étant par défaut respectueuse de la vie privée. Les commissaires à la protection des données et à la vie privée ont réaffirmé leur volonté de renforcer leur coopération et de poursuivre leurs efforts en vue de l'adoption d'un instrument international contraignant au niveau mondial. À cet effet, ils ont adopté deux résolutions. La première vise à mettre en place une structure de coopération au sein de la conférence internationale et donne mandat à un groupe de travail de faire des propositions en ce sens en 2011. La deuxième appelle les gouvernements du monde entier à tenir une conférence intergouvernementale en vue de parvenir à un accord sur un tel instrument international (voir sur notre site www.leprepose.ch , sous Thèmes – Protection des données – Coopération internationale). Dans cette résolution, les commissaires soutiennent également «activement les initiatives tendant à trouver des solutions appropriées pour continuer à assurer la protection effective des droits et libertés fondamentaux et l'exercice de ces droits, notamment le droit à la vie privée lors du traitement de données à caractère personnel». Les commissaires ont également adopté une résolution consacrée au principe du développement conforme à la protection des données dès la conception de systèmes, de services ou de produits («privacy by design»).

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

Au cours de l'année écoulée, le Groupe de travail sur la sécurité de l'information et de la vie privée s'est penché sur les innovations techniques permettant l'enregistrement et l'exploitation d'énormes quantités de données personnelles au-delà des frontières, ainsi que sur la révision des directives sur la sécurité et la protection des données. Il a également abordé le développement des signatures numériques, la protection des enfants et des jeunes sur Internet et la mise en œuvre transfrontière des dispositions juridiques en matière de protection des données.

Nul ne contestera que le développement d'Internet a modifié de manière aussi rapide que radicale le traitement des données personnelles. Aujourd'hui, on peut enregistrer et évaluer à volonté un volume de données jusque-là impensable. Ces énormes quantités de données sont traitées grâce à des procédés techniques permettant presque tout ce que l'on peut imaginer comme exploitation de données. En outre, il est possible de traiter et d'enregistrer ces données en tout point du monde et souvent à l'insu des personnes concernées. Cette situation soulève des questions difficiles sur le droit applicable et la mise en œuvre des prétentions juridiques. La sphère privée est placée devant des défis jusqu'ici jamais rencontrés qu'il convient de relever dans un contexte désormais mondial.

Face à cette situation, le groupe de travail a proposé d'examiner si les directives de l'OCDE, établies il y a 30 ans, répondent aujourd'hui aux données actuelles en matière de sécurité et de protection des données. Au cours de l'année écoulée, un rapport d'expert soulignant les nouveaux enjeux a été publié. Il s'agit maintenant de vérifier si les huit principes à la base des directives sont encore valables. Un questionnaire présentant un certain nombre de propositions de révision a été envoyé aux pays membres.

Dans le domaine de la gestion de l'identité et des signatures numériques, un rapport comparatif a été présenté à propos des modèles actuels de gestion de l'identité. Le modèle autrichien y figure comme étant la solution optimale en matière d'identification numérique, mais aussi comme modèle de base pour les applications de gouvernance électronique. De plus, ce rapport souligne l'absence d'interopérabilité des systèmes, ce qui constitue l'obstacle majeur à la percée de ces applications malgré les quelques progrès accomplis.

Durant la même période, le groupe de travail a présenté deux rapports sur les responsabilités des fournisseurs de services de télécommunication. Aucune unité de vue ne règne actuellement parmi les pays membres, comme l'a permis de constater l'examen de ces responsabilités. Les avis divergent actuellement en ce qui concerne la possibilité

d'imposer aussi aux opérateurs de services des tâches étatiques de surveillance et de contrôle (lutte contre la piraterie, la pédophilie, etc.). Deux points de vue se dessinent: l'un penche pour une formulation détaillée des responsabilités des opérateurs de services d'accès à Internet, l'autre préfèrerait aborder le problème par le biais de l'autorégulation. Ce thème occupera les discussions pendant un certain temps encore, car les démarches nationales diffèrent largement; mais pour l'économie et les utilisateurs, il serait judicieux que l'on trouve une solution commune.

Un volumineux rapport a été présenté sur la protection des enfants et des jeunes sur Internet. Il a été complété par des informations émanant des pays membres et devrait être publié l'année prochaine. Certains pays sont d'avis que la protection des enfants et des jeunes sur Internet requiert l'élaboration d'une directive de l'OCDE.

Un site web a été créé par l'OCDE pour la mise en œuvre et la simplification de la coopération transfrontalière et pour l'application du droit en matière de protection des données (Global Privacy Enforcement Network, GPEN). Les autorités de protection des données de la Suisse et de plusieurs autres pays (dont la France, l'Allemagne, l'Italie, l'Espagne, le Canada et les États-Unis) y collaborent. L'échange informel d'informations entre les autorités se heurte toutefois à des limites car les lois nationales ne le permettent pas sans autre.

Enfin, au cours de l'année écoulée, les candidatures du Chili, d'Israël, de l'Estonie et de la Slovénie ont été examinées et approuvées par le Conseil des ministres. Le Conseil entend par ailleurs mettre en place une coopération plus étroite avec les pays à forte croissance économique comme le Brésil ou l'Inde.

Association francophone des autorités de protection des données

L'Association francophone des autorités de protection des données (AFAPDP) a tenu sa 4e conférence à Paris, le 30 novembre 2010. Elle a été suivie de l'Assemblée générale de l'association et d'un séminaire de formation pour les membres des autorités francophones de protection des données. La conférence a notamment abordé les développements du droit de la protection au plan international et au sein des pays membres de la Francophonie. Nous avons ainsi présenté le rôle de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans l'optique de l'adoption d'un instrument juridique universel.

L'AFAPDP a adopté deux résolutions. La première a trait à la promotion de l'usage de la langue française comme langue de travail officielle dans les instances internationales. L'association est d'avis que le caractère multilatéral et multilingue doit être préservé dans les différentes instances internationales et en particulier au sein de la conférence internationale des commissaires à la protection des données. La seconde résolution

concerne la promotion de «l'adoption de législations relatives à la protection des données et l'établissement d'autorités indépendantes de contrôle dans les États francophones qui en sont dépourvus», ainsi qu'un soutien aux «initiatives visant à adopter ou modifier un instrument international contraignant sur le respect de la vie privée et la protection des données et visant à renforcer la coopération internationale entre les autorités de protection des données». En particulier, l'association soutient la tenue d'une conférence intergouvernementale en vue de favoriser le développement d'un tel instrument international. Nous avons également apporté une contribution active au séminaire de formation, notamment en animant deux ateliers consacrés aux principes de base de la protection des données et à l'organisation et au fonctionnement des autorités de protection des données.

2. Loi sur la transparence

2.1 Demandes d'accès

2.1.1 Départements et offices fédéraux

En 2010, le nombre des demandes d'accès déposées est encore dans la moyenne des années précédentes. Depuis l'entrée en vigueur du principe de la transparence, deux tendances apparaissent: d'une part, le refus total de l'accès est prononcé dans toujours moins de cas, d'autre part l'accès au moins partiel est de plus en plus fréquemment accordé. Dans un bon quart des cas dans lesquels l'administration a accordé un accès restreint, une demande en médiation a été déposée.

Selon les chiffres qui nous ont été communiqués, 239 demandes d'accès ont été déposées auprès des autorités fédérales en 2010. Dans 106 cas, les autorités ont accordé un accès complet et dans 63 cas un accès partiel. Dans 62 cas, l'accès aux documents a été totalement refusé. Huit cas ont été annoncés comme pendants. Ces chiffres n'ont pas notablement changé par rapport aux années précédentes (voir la statistique figurant au chiffre 3.7).

Ces chiffres permettent à nouveau de tirer une conclusion positive: depuis l'entrée en vigueur de la loi sur la transparence (LTrans), le pourcentage des refus complets est en diminution constante. Il était de 43% en 2006, de 33% en 2007, de 32% en 2008, de 29% en 2009 et de 26% en 2010. Pour ce qui est des accès partiels, leur proportion est passée en un an de 17% (2009) à 26% en 2010, ce qui constitue le pourcentage le plus élevé jamais enregistré. En revanche, les accès entièrement accordés en 2010 représentent «seulement» 44% de tous les cas, ce qui constitue le chiffre le plus bas depuis l'entrée en vigueur de la loi sur la transparence (moyenne des années précédentes: 54%).

Il est intéressant de noter les grandes différences quant au nombre de demandes d'accès annoncées par les autorités fédérales. Ainsi, l'OFSP a par exemple annoncé 32 demandes d'accès. Par contre, 20 autorités fédérales nous ont informés qu'elles n'avaient reçu en 2010 aucune demande d'accès. Cela montre à nouveau que la pertinence de ce genre de chiffres est limitée. Il n'y a toujours pas de saisie systématique des demandes d'accès. En outre, on suppose que dans la majorité des cas, les demandes ne sont pas reconnues en tant que demandes d'accès conformément à la loi sur la transparence. En réalité, le nombre des demandes d'accès est probablement bien plus élevé.

En 2010, dans 8 cas, un émolument a été demandé à la personne ayant déposé la demande d'accès (6 cas en 2009). Le montant total des émoluments encaissés qui nous a été communiqué (3460 francs) est à peine inférieur à celui de l'année précédente (3850 francs). Sur la base des demandes en médiation déposées, on peut toutefois constater que certains offices ont commencé à requérir des émoluments considérablement plus élevés.

Les offices et les départements ne sont pas tenus de consigner le temps consacré au traitement des demandes d'accès et à la participation en cas de procédure de médiation. En outre, selon les départements, ce temps n'est pas saisi de manière uniforme. Les données qui nous ont été transmises sur une base volontaire ne sont donc pas forcément significatives. Selon celles-ci, la charge de travail a de nouveau augmenté (2007: 273 heures; 2008: 509 heures; 2009: 748 heures; 2010: 815 heures).

Les conseillers à la transparence des offices et des départements estiment que leur charge de travail occasionnée par l'application de la loi sur la transparence (demandes d'accès, procédures de médiation, formation interne au niveau de l'office, accompagnement législatif, etc.) est très diverse. Certains la considèrent comme étant plutôt réduite, d'autres, en particulier ceux traitant dans leur office des thèmes importants de politique économique et sociale, font état d'un volume de travail considérable. Tous s'accordent à dire que l'audition de tiers et surtout la participation aux procédures de médiation impliquent très rapidement une importante charge de travail.

2.1.2 Services parlementaires

Selon les informations fournies par les services parlementaires, aucune demande d'accès ne leur a été transmise en 2010.

2.2 Demandes en médiation

En 2010, nous avons reçu en tout 32 demandes en médiation (voir la statistique au chiffre 3.9). L'année précédente, elles étaient au nombre de 41. En tout, 34 demandes en médiation ont été réglées. Dans 10 cas, une solution consensuelle a été trouvée avec les parties impliquées. Dans 14 cas, où une solution à l'amiable n'a pas pu être trouvée ou n'était pas envisageable d'emblée, nous avons émis des recommandations. Plusieurs demandes en médiation ont pu être réglées par une seule recommandation ou en une seule médiation. En cours de procédure de médiation, dans un cas la demande a été retirée et dans un autre l'autorité a accordé d'elle-même l'accès demandé. Dans trois cas, l'accès a été demandé pour des documents qui ne relevaient pas du champ d'application personnel de la loi sur la transparence. Il est intéressant de noter que toutes ces demandes ont été déposées par des avocats. Dans un cas, la demande en médiation n'a pas été remise dans les délais.

Ces chiffres permettent d'émettre quelques remarques et de tirer les conclusions suivantes:

Dans 125 cas, les autorités ont entièrement refusé l'accès (62) ou ne l'ont accordé que partiellement (63). Suite à ces refus complets ou partiels, 32 demandes en médiation ont été déposées chez nous. Cela signifie donc que dans presque 26% des accès entièrement ou partiellement refusés, nous avons reçu par la suite une demande en médiation. L'année précédente, ceci était encore le cas pour 38% des refus.

Dans deux tiers des procédures de médiation menées à terme (médiations et recommandations), nous avons à nouveau réussi à trouver une solution plus favorable pour le demandeur, à savoir une médiation ou un accès plus étendu que celui qui avait été accordé à l'origine par l'office fédéral.

Un fait demeure inchangé, à savoir le retard important accumulé dans le traitement des demandes d'accès, fait d'autant plus regrettable qu'il se traduit pour les demandeurs par un long délai d'attente jusqu'aux procédures de médiation. Cette année encore, le Tribunal administratif fédéral a reproché au préposé fédéral un déni de justice (retard injustifié) (arrêt du 1er mars 2010, A-363/2010).

2.3 Procédures de médiation closes

2.3.1 Recommandations

Les recommandations émises au cours de l'année sous revue concernant la loi sur la transparence sont résumées ci-dessous. La version complète de ces recommandations peut être consultée sur notre site web www.leprepose.ch, sous la rubrique Documentation – Principe de la transparence – Recommandations. Deux recommandations importantes sont reproduites in extenso en annexe, au chiffre 4.2.

Recommandation OFSP – CFV / Déclarations d'intérêts (12 février 2010)

La demanderesse a requis l'accès aux déclarations d'intérêts des membres de la Commission fédérale pour les vaccinations (CFV) et du groupe de travail «Vaccination contre les papillomavirus humains». L'Office fédéral de la santé publique (OFSP), qui gère le secrétariat de la CFV, a refusé l'accès aux documents en question en se référant au message du Conseil fédéral selon lequel les commissions consultatives ne tombent pas dans le champ d'application de la loi sur la transparence. Dans sa recommandation, le préposé fédéral a souligné que conformément à l'ordonnance sur l'organisation du gouvernement et de l'administration, les commissions extraparlementaires, dont font également partie les commissions consultatives, sont subordonnées à l'administration fédérale et que le principe de la transparence leur est également applicable. Il a recommandé d'accorder l'accès aux déclarations d'intérêts en raison d'un intérêt public prépondérant (protection de la santé publique). La recommandation figure dans son intégralité au chiffre 4.2.1 (uniquement en allemand).

Recommandation OFAS / Liste de contrôle AI I + II (16 mars 2010)

Indépendamment l'un de l'autre, deux demandeurs ont requis l'accès à la liste de contrôle AI que l'Office fédéral des assurances sociales (OFAS) a soumis aux services cantonaux de l'AI, accompagnée d'une stratégie de lutte contre la fraude. L'OFAS a refusé l'accès à l'ensemble de la liste au motif qu'il pourrait entraver la mise en œuvre conforme aux objectifs de mesures concrètes décidées par une autorité, à savoir le tri efficace d'abus possibles à l'AI. Le préposé fédéral ne s'est pas rangé à cet avis. D'une part, de grands extraits de la liste de contrôle sont depuis longtemps connus du public (et pourtant l'OFAS n'a pas retiré la liste). D'autre part, le préposé fédéral n'a pas qualifié l'utilisation de la liste de contrôle AI de mesure concrète d'une autorité. Il estime qu'elle constitue une simple liste de questions standard utilisée par les spécialistes internes de l'AI en matière de fraude pour détecter les possibles cas d'abus. La publication de la liste n'a pas pour conséquence un risque de dommages grave. Le préposé

a donc recommandé d'accorder l'accès de l'ensemble de la liste de contrôle AI. La recommandation «Liste de contrôle AI I» figure dans son intégralité au chiffre 4.2.2 (uniquement en allemand).

Voir également le chiffre 2.4.1 du présent rapport d'activités.

Recommandation DDPS / Grade et fonction (26 mars 2010)

Le demandeur s'est adressé au Département fédéral de la défense, de la protection de la population et des sports (DDPS) pour savoir si des extrémistes de droite servent dans l'armée suisse comme officiers. Il a joint à sa demande une liste de noms de personnes et désirait savoir si ces personnes avaient le grade de sous-officier ou d'officier. Ces informations figurent dans le Système d'informations sur le personnel de l'armée (SIPA). Or le DDPS a refusé au demandeur l'accès aux extraits du SIPA en invoquant des motifs de protection des données. Le préposé fédéral est également parvenu à la conclusion que dans le cas concret, les informations demandées ne peuvent être communiquées ni en vertu d'une disposition spéciale, ni en se fondant sur la loi sur la transparence ou sur la loi sur la protection des données. Il a donc recommandé au DDPS de ne pas accorder l'accès aux extraits du SIPA.

Recommandation Swissmedic / Dossiers d'autorisation (30 mars 2010)

Deux demanderesses se sont adressées à Swissmedic pour obtenir l'accès à de nombreux documents traitant de la mise de médicaments sur le marché. Ayant envisagé d'accorder un accès partiel aux dossiers d'autorisation, l'Institut Swissmedic a entendu les entreprises pharmaceutiques concernées. Ces dernières se sont prononcées contre l'octroi de l'accès en invoquant d'une part les secrets d'affaires et de fabrication et d'autre part la protection de leur sphère privée. Du fait que Swissmedic maintenait son intention de donner partiellement accès aux dossiers, les demanderesses et les entreprises concernées ont déposé des demandes en médiation. Le préposé fédéral a évalué la démarche et l'appréciation de Swissmedic quant à la présence de secrets de fabrication et d'affaires et à la protection de données personnelles de tiers comme étant conformes à la loi et appropriées. Il a recommandé à Swissmedic de maintenir sa proposition d'autoriser un accès partiel aux dossiers. Le texte intégral de la recommandation figure en annexe au chiffre 4.2.3.

Recommandation OFJ / Loterie Romande (28 avril 2010)

Le demandeur a déposé auprès du l'Office fédéral de la justice (OFJ) une demande d'accès aux «chiffres des billets non vendus de la Loterie Romande» de l'année 2008. L'OFJ a répondu que le nombre de billets non vendus ne lui avait malheureusement pas été fourni. Le préposé fédéral a constaté dans sa recommandation que la loi sur

la transparence s'applique uniquement à des documents qui sont détenus par l'autorité dont ils émanent ou à laquelle ils ont été communiqués. En d'autres termes, le requérant ne peut pas exiger sur la base de la loi sur la transparence que l'OFJ établisse un document. Le texte intégral de la recommandation figure en annexe au chiffre 4.2.4.

Recommandation OFSP / Accès aux contrats concernant les vaccins pandémiques (12 mai 2010)

Le demandeur a requis l'accès à trois contrats (vente de vaccins pandémiques) que la Confédération avait conclus avec deux entreprises pharmaceutiques. L'Office fédéral de la santé publique (OFSP) a accordé l'accès partiel aux contrats, dont un avait déjà fait deux fois l'objet d'une recommandation du préposé fédéral. Celui-ci a estimé comme l'OFSP que les contenus des contrats étaient des secrets d'affaires et de fabrication, à l'exception d'une page d'un contrat, qui est déjà connue du public.

Recommandation Office fédéral de l'agriculture / Extension de la liste des produits phytosanitaires non soumis à autorisation (8 juin 2010)

Une entreprise a demandé à l'Office fédéral de l'agriculture (OFAG) de pouvoir consulter deux lettres dans lesquelles des réserves avaient été levées dans le cadre d'une procédure concernant l'admission de produits dans la liste des produits phytosanitaires non soumis à autorisation. L'office avait l'intention d'accorder l'accès partiel aux deux lettres et a auditionné pour cela la tierce personne concernée. Celle-ci était en principe d'accord de permettre l'accès partiel aux deux lettres, mais désirait caviarder un passage qui renfermait des données personnelles sur une autre tierce personne. Le préposé fédéral a partagé l'avis de l'OFAG sur l'appréciation du secret d'affaires et sur l'absence de garantie du secret si des informations étaient communiquées. Le préposé a suggéré néanmoins à propos du passage en question de procéder à une audition de la tierce personne concernée.

Recommandation Office fédéral de la justice / Fax envoyé aux États-Unis dans l'affaire Roman Polanski (9 juin 2010)

Le demandeur a demandé à l'Office fédéral de la justice (OFJ) l'accès au fax que l'OFJ avait envoyé à l'Office of International Affairs le 21 septembre 2009 concernant Roman Polanski, ainsi qu'aux documents qui avaient abouti à l'envoi de ce fax et qui se référaient à son contenu. L'OFJ a refusé d'accorder l'accès en argumentant que les documents demandés faisaient partie d'une procédure d'entraide judiciaire internationale. Le préposé fédéral s'est rangé à cette appréciation dans sa recommandation et a retenu que la loi sur la transparence n'est pas applicable à l'accès à des documents d'une procédure d'entraide judiciaire internationale.

Recommandation DDPS / Rapport «Imams islamistes» (21 octobre 2010)

Deux journalistes ont demandé au Département fédéral de la défense, de la protection de la population et des sports (DDPS) l'accès au rapport intitulé «Imams islamistes», établi par l'État-major de la Délégation du Conseil fédéral pour la sécurité. Le DDPS a informé les demandeurs que le rapport était classé confidentiel et a refusé d'en accorder l'accès qui aurait pu menacer la sécurité intérieure ou extérieure ou porter atteinte aux intérêts de politique extérieure ou aux relations internationales de la Suisse. Le préposé fédéral n'a pas partagé cette appréciation et a donc recommandé d'accorder l'accès à de larges parties du rapport. Le texte intégral de la recommandation figure en annexe au chiffre 4.2.5 (uniquement en allemand).

Recommandation DDPS / Rapport d'inspection de la Surveillance des services de renseignement (18 novembre 2010)

Un journaliste a déposé auprès du Département fédéral de la défense, de la protection de la population et des sports (DDPS) une demande d'accès à deux rapports d'inspection de la Surveillance des Services de renseignement du DDPS, concernant la protection de l'État. Le DDPS a refusé l'accès en argumentant que les rapports d'inspection étaient classés confidentiels et servaient aux autorités de surveillance de base de décision pour d'autres mesures. En outre, il a estimé que fournir l'accès à ces documents était susceptible de porter atteinte à la sécurité de la Suisse, aux intérêts de politique étrangère du pays et aux relations entre la Confédération et les cantons. Le préposé fédéral a fait observer au DDPS que la loi sur la transparence n'était pas applicable aux rapports d'inspection établis sur mandat direct et particulier de la Délégation des Commissions de gestion et de ce fait explicitement qualifiés de confidentiels conformément à la loi sur le Parlement. Pour ce qui était du second rapport d'inspection, le préposé s'est rangé à l'argumentation du DDPS selon laquelle l'accessibilité totale du rapport pourrait compromettre sérieusement la sécurité intérieure et extérieure de la Suisse. Le préposé en a donc recommandé une publication partielle.

Recommandation DFAE / Interview autorisée (9 décembre 2010)

Le demandeur a requis auprès du Département fédéral des affaires étrangères (DFAE) l'accès à des documents en rapport avec une interview que la cheffe de département avait accordée à un quotidien. Le DFAE a rejeté la demande d'accès en argumentant que les documents n'avaient pas atteint leur stade définitif d'élaboration et qu'ils étaient destinés à un usage personnel. Le département a estimé en effet que seule l'interview autorisée publiée dans le quotidien est un document définitif. Par contre, pour

le préposé fédéral, le document terminé est non pas l'interview publiée, mais déjà le document contenant l'interview autorisée car il représente l'étape de travail ultime et définitive de l'activité administrative. Il a recommandé au DFAE d'accorder l'accès à ce document.

Recommandation DFAE / Accréditation d'un ambassadeur (22 décembre 2010)

Le demandeur a requis auprès du Département fédéral des affaires étrangères (DFAE) l'accès aux lettres de créance de l'ambassadeur d'Allemagne en Suisse, ainsi que des copies de son passeport diplomatique. Le DFAE a refusé au motif que si l'on permettait l'accès à des documents remis sous le sceau de la confidentialité par un autre État conformément à l'usage diplomatique, cela porterait atteinte d'une manière très générale aux relations avec d'autres États et plus particulièrement aux relations avec l'Allemagne. Le préposé fédéral n'a par contre pas estimé que rendre accessibles les lettres de créance se traduirait par une atteinte aux relations avec l'Allemagne et a recommandé d'en accorder l'accès. Il a refusé la publication des copies du passeport diplomatique pour des motifs de protection des données.

Recommandation OFAG / Groupe de travail constitué par le Département fédéral de l'économie (23 décembre 2010)

La demanderesse a requis auprès de l'Office fédéral de l'agriculture (OFAG) l'accès à une liste de 250 propositions (Synopsis) du groupe de travail «Mesures d'accompagnement Accord de libre échange». L'OFAG a refusé en argumentant que le groupe de travail n'appartenait pas à l'administration fédérale et n'était donc pas soumis à la loi sur la transparence. Il a ajouté que le groupe de travail avait décidé de ne pas publier de résultats intermédiaires. Dans sa recommandation, le préposé fédéral a souligné essentiellement deux points fondamentaux: d'une part tous les groupes de travail institués par l'administration fédérale sont soumis à la loi sur la transparence; d'autre part, les services soumis à la loi sur la transparence (départements, offices, tous les groupes de travail et d'experts, experts individuels, etc.) ne peuvent, de leur propre compétence, exclure de la loi sur la transparence les documents qu'ils établissent; ceux-ci doivent donc être appréciés conformément aux dispositions de cette loi. Au terme d'une audience de médiation, le préposé a qualifié le document «Synopsis» de document officiel et a recommandé de le rendre accessible sous forme anonymisée. Le texte intégral de la recommandation figure en annexe au chiffre 4.2.5.

2.3.2 Médiations

Nous avons trouvé une solution consensuelle dans les cas suivants:

Médiation OFSP / Contrats H1N1

Le demandeur a prié l'Office fédéral de la santé publique (OFSP) de lui remettre des copies des contrats concernant l'achat de vaccins pandémiques. Les autorités n'ayant pas pris position dans le délai légal, le demandeur a déposé une demande en médiation. L'OFSP a remis les contrats sur intervention du préposé fédéral.

Médiation OFS / Rapport sur la Statistique suisse des prix du terrain

Le demandeur a prié l'Office fédéral de la statistique (OFS) de lui remettre un rapport sur la consultation relative à la Statistique suisse des prix du terrain datée de mai 1997. L'OFS a informé le demandeur que le document avait été établi avant l'entrée en vigueur de la loi sur la transparence et, de ce fait, n'était pas accessible («secret de fonction»). Sur intervention du préposé fédéral, l'OFS s'est déclaré prêt à remettre malgré tout le rapport au demandeur.

Médiation SAS / Rapport d'audit

Le demandeur a requis auprès du Service d'accréditation suisse (SAS) l'accès à un rapport d'audit. Au cours d'une audience de médiation organisée par le préposé fédéral, les participants se sont accordés sur la suite de la procédure, notamment sur l'audition de la tierce personne concernée.

Médiation OFT / Rapport d'experts sur les nuisances dues au bruit causées par les chemins de fer portuaires

La demanderesse a requis auprès de l'Office fédéral des transports (OFT) l'accès à un rapport d'experts qui traitait des nuisances dues au bruit provoqué par l'exploitation des chemins portuaires (à Bâle) à l'égard des riverains. L'OFT n'a pas réagi à la demande d'accès de la demanderesse. Sur intervention du préposé fédéral, le rapport a été immédiatement remis à la demanderesse.

Médiation OFIT / Liste des fichiers

Le demandeur a requis auprès de l'Office fédéral de l'informatique et de la télécommunication (OFIT) l'accès à une liste de fichiers gérés par l'OFIT sur mandat de tiers et de fichiers exploités par l'OFIT lui-même. Dans un cas, l'OFIT a refusé l'accès demandé

et a communiqué au demandeur le montant des émoluments dus. Sur intervention du préposé fédéral, le demandeur s'est vu remettre les listes souhaitées sans frais.

Médiation DFAE / Directives sur les visas pour la Libye

Le demandeur a requis la publication des directives concernant l'octroi de visas pour les ressortissants libyens; invoquant les problèmes dans les relations entre la Suisse et la Libye, le Département fédéral des affaires étrangères (DFAE) a répondu par la négative.

Au cours de la procédure de médiation, les participants ont convenu que le DFAE examinerait à nouveau la question de la remise des directives soit après la publication du rapport de la Commission de gestion parlementaire sur le dossier «Libye», soit après clôture de la procédure d'arbitrage.

Médiation OFAC / Audits et rapports d'inspection

Le demandeur a requis l'accès au système de gestion d'affaires et l'établissement d'une liste détaillée, sous forme électronique, des audits et inspections des unités Sécurité technique, Sécurité des opérations aériennes et Sécurité des infrastructures. L'Office fédéral de l'aviation civile (OFAC) a refusé en argumentant notamment que la demande n'était pas formulée de manière assez précise. Sur la suggestion du préposé fédéral, l'OFAC a établi une liste des audits et inspections réalisés. Le demandeur s'est déclaré satisfait de cette démarche.

Médiation SER / Recherche dans le domaine aéronautique

Le demandeur a requis l'accès à de nombreux documents concernant la coopération internationale dans le domaine aéronautique. Après la remise de la demande en médiation, le Secrétariat d'État à l'éducation et à la recherche (SER) est resté en contact avec le demandeur. Par la suite, ce dernier a informé le préposé fédéral que du fait de l'évolution positive des pourparlers avec le SER, un terme pouvait être mis à la procédure de médiation.

Médiation OFEV / Allégement fiscal écobilan des carburants

Le demandeur a requis l'accès aux documents concernant les demandes d'allègements fiscaux en relation avec l'ordonnance sur l'écobilan des carburants. L'Office fédéral de l'environnement (OFEV) a informé le demandeur que la procédure d'examen n'était pas encore terminée et a en outre déclaré qu'un accès ne pouvait pas être accordé en raison des secrets d'affaires et de la nécessité de protéger les données personnelles. Durant l'audience de médiation à laquelle participait aussi la Direction

générale des douanes (DGD), chargée de prendre la décision définitive concernant les allègements fiscaux, il est apparu que le demandeur ne voulait pas consulter tous les dossiers, mais seulement certaines informations. Les deux offices ont délivré les renseignements demandés et le demandeur s'est déclaré très satisfait du résultat.

Médiation OFS / Expertise du service des méthodes

La demanderesse a requis l'accès à l'expertise du service des méthodes de l'OFS concernant la représentativité du Dépouillement centralisé des données comptables. Sur intervention du préposé fédéral, l'OFS est revenu sur sa décision première et a remis à la demanderesse l'expertise souhaitée.

2.4 Arrêts des tribunaux relatifs à la loi sur la transparence

2.4.1 Tribunal administratif fédéral

Le Tribunal administratif fédéral (TAF) a jugé que la liste de contrôle IV de l'Office fédéral des assurances sociales (OFAS) doit être accessible au public. Ce faisant, le tribunal s'est rangé à l'argumentation développée par le préposé dans sa recommandation du 16 mars 2010. D'après l'arrêt du TAF, il est improbable que la liste de contrôle standard ne puisse plus être utilisée comme outil de travail après sa publication. Le tribunal ne s'est donc pas rangé à l'avis de l'OFAS, qui estimait que la publication de la liste de contrôle mettait sérieusement en danger la découverte de possibles abus à l'AI, mais à la recommandation du préposé fédéral (cf. arrêt du TAF du 18 octobre 2010, réf. A-3269/2010).

À la suite d'une recommandation élaborée par le préposé fédéral en date du 22 avril 2009 à l'intention de l'OFSP (cf. notre 17e rapport d'activités 2009/2010, chiffre 2.3.1), le TAF a précisé que les documents établis par l'administration en vue de la préparation d'une proposition au Conseil fédéral ne relevaient pas de la procédure de co-rapport, laquelle est exclue de la loi sur la transparence. Ainsi, les documents élaborés afin de préparer au niveau administratif interne une proposition ou une décision avant la procédure de co-rapport, relèvent du principe de la transparence, indépendamment du fait que l'administration les ait établis elle-même ou les ait reçus de tiers. Ces documents sont en principe accessibles même s'ils ont été joints à la proposition au Conseil fédéral (cf. arrêt du TAF du 3 mai 2010, réf. A-4049/2009).

En 2010, le Tribunal administratif fédéral a de nouveau reproché au préposé fédéral un déni de justice (retard injustifié, arrêt du TAF du 1er mars 2010, réf. A-363/2010).

2.4.2 Tribunal fédéral

Dans son arrêt du 19 mai 2010 (réf. 1C_522/2009), le Tribunal fédéral a défini les documents officiels qui constituent l'objet d'une procédure de co-rapport. Dans le cas concret, il s'agissait des conventions relatives à la dissolution des rapports de travail (conventions de départ) de l'ancien secrétaire général du Département fédéral de justice et police et de son suppléant. Dans un arrêt précédent, le Tribunal administratif fédéral avait estimé que ces conventions, en tant que partie d'une proposition au Conseil fédéral, devaient être qualifiées de documents relevant de la procédure de co-rapport et, de ce fait, demeuraient confidentielles au regard de la loi sur la transparence.

Le TF a maintenant établi que cette disposition est à interpréter de manière restrictive: ne font partie de la procédure de co-rapport que les documents qui sont établis

entre la signature de la proposition au Conseil fédéral par le chef de département et la décision du Conseil fédéral. Indirectement, le TF a de ce fait également jugé que les conventions de départ des hauts fonctionnaires de la Confédération sont, en principe, accessibles au public. En outre, il a souligné que la transparence est désormais la règle et que le secret n'est plus possible que dans les cas d'exception. Il a annulé le jugement attaqué et a enjoint l'instance inférieure de juger à nouveau le cas en procédant à la pesée des intérêts. Le Tribunal administratif fédéral est à présent arrivé à la conclusion que l'intérêt du demandeur – et plus généralement l'intérêt public – à l'accès aux conventions de départ prime sur la protection de la sphère privée des personnes concernées. Les documents concernés sont donc publiquement accessibles (cf. arrêt du TAF du 17 février 2011, réf. A3609/2010. Le préposé fédéral était arrivé à la même conclusion dans sa recommandation du 9 février 2009 (cf. notre 17e rapport d'activités 2009/2010, chiffre 2.3.1).

2.5 Consultation des offices

2.5.1 Révision de la loi sur les denrées alimentaires

Le préposé fédéral s'est prononcé sur la révision de la loi sur les denrées alimentaires. Conformément au projet, certains documents relevant de domaines précis ne doivent pas être soumis au principe de la transparence. Toutefois, de l'avis du préposé, il existe toujours des motifs pertinents en faveur d'une plus large transparence. Si le législateur devait se prononcer pour une disposition spéciale au sens de l'art. 4 LTrans, il serait de l'avis du préposé nécessaire de définir de manière claire et nette au niveau du contenu les différents documents officiels qui doivent être soustraits de la loi sur la transparence. Ce n'est qu'ainsi que les consommateurs seraient clairement informés qu'ils n'ont pas de droit d'accès à certaines informations (comme les rapports de contrôle et de test).

En outre, le projet prévoyait une disposition portant le titre «Devoir de discrétion» selon laquelle toutes les personnes exerçant des fonctions officielles devaient être soumises au secret de fonction. Selon le rapport explicatif, cette obligation avait en premier lieu pour but de garantir la discrétion des mandataires externes. Le préposé a souligné dans ce contexte que cette disposition sur le devoir de discrétion n'avait pas d'autre but que d'étendre aussi le champ d'application du secret de fonction conformément à l'art. 22 LPers à des personnes externes à l'administration. Étant donné que le secret de fonction a été redéfini quant à sa portée par l'entrée en vigueur de la loi sur la transparence, il ne porte (plus) aujourd'hui que sur des informations qui ne relèvent pas du champ d'application de la loi sur la transparence, qui sont rendues secrètes par l'application de la législation spéciale ou qui tombent sous le coup d'une des exceptions prévues dans la loi sur la transparence elle-même. Ni le secret de fonction, ni la disposition sur le devoir de discrétion prévue dans le projet de loi sur les denrées alimentaires ne constituent donc une disposition spéciale au sens de l'art. 4 LTrans. En outre, le préposé souligne que la loi sur la transparence prévoit les mesures nécessaires permettant de protéger les secrets d'affaires et de fabrication, ainsi que la sphère privée et les données personnelles de tiers et qu'à son avis, le devoir de discrétion sous la forme proposée n'est pas nécessaire.

2.5.2 Protection de l'information

Dans le cadre de la consultation des offices relative au rapport du Conseil fédéral sur l'application de l'ordonnance concernant la protection de l'information et à la création d'une base légale formelle de la protection des informations, le préposé fédéral a exprimé des doutes sur le fait que la création de cette base ne soit pas contestée au sein de l'administration. En outre, il a précisé d'une part que le besoin d'élargir la protection de

l'information n'avait pas été développé de manière convaincante et d'autre part qu'en créant la loi sur la transparence, le législateur avait clairement signalé que l'administration fédérale devait axer son action sur la transparence. Le préposé fédéral s'est donc montré surpris de l'ampleur avec laquelle la protection de l'information dans l'administration, notamment dans le secteur civil, devait à nouveau être renforcée. Enfin, il reproche le fait que les considérations relatives à la loi sur la transparence soient peu précises et infondées à divers égards.

3. Le PFPDT

3.1 Evaluation de la loi fédérale sur la protection des données

L'Office fédéral de la justice (OFJ) a chargé le Büro Vatter AG, l'Institut de droit européen de l'Université de Fribourg et l'Institut de sondage Demoscope SA de procéder à une évaluation de l'efficacité de la loi fédérale sur la protection des données. Pour accompagner le travail d'évaluation, l'OFJ a mis en place un groupe de travail composé de représentants de l'administration fédérale, du PFPDT, des autorités cantonales de protection des données et de l'économie, ainsi que d'experts indépendants. Le rapport d'évaluation devrait être rendu public dans le courant 2011. Cette évaluation pourrait déboucher sur une révision de la LPD. Elle donne l'occasion au PFPDT de s'interroger sur la pertinence du droit actuel et de formuler quelques pistes de réflexion.

L'évaluation de la LPD menée par le Büro Vatter AG avec la collaboration de l'Institut de droit européen de l'Université de Fribourg et l'Institut de sondage Demoscope SA a pour objectif d'analyser l'effectivité et l'efficacité de certaines dispositions de la loi, le cas échéant, de faire des propositions de modifications. L'évaluation met l'accent principalement sur la connaissance de la loi et sur les mécanismes de mise en œuvre. En particulier, les évaluateurs examinent dans quelle mesure les droits des personnes concernées et la procédure pour faire valoir ces droits permettent effectivement et de manière adéquate de garantir le respect des droits fondamentaux et de la vie privée. L'évaluation porte également sur le rôle, les tâches et les compétences du Préposé fédéral à la protection des données et à la transparence. Les résultats de cette évaluation devraient être rendus publics dans le courant de l'année 2011. Cette évaluation permet également une réflexion sur la pertinence du droit actuel pour répondre aux défis des technologies de l'information et des communications.

La loi fédérale à la protection des données est une loi-cadre qui couvre l'ensemble des traitements de données personnelles, quels que soient la nature et le mode de traitement des données. Elle est technologiquement neutre. Même si les principes fondamentaux de la protection des données énoncés aux articles 4 et suivants demeurent pertinents et applicables aux technologies actuelles de traitement des données, il est légitime de s'interroger sur l'effectivité de la loi eu égard aux nouvelles technologies de l'information et de la communication basées en particulier sur l'ubiquité, la surveillance, la géolocalisation, la miniaturisation, la proximité (Internet des choses), le profilage, le traçage et le contact permanent. L'individu a de moins en moins d'opportunités de vivre seul à l'abri de tout regard et tous ses faits et gestes sont susceptibles

d'être enregistrés, analysés et exploités. L'individu est non seulement sujet du traitement des données personnelles le concernant, mais également responsable de traitement, notamment au travers de l'utilisation des réseaux sociaux. S'il est conscient de l'importance de l'information et apprécie les avantages et les potentialités des technologies actuelles, il n'en mesure souvent pas suffisamment les risques et est de moins en moins à même de maîtriser l'information qui le concerne. Le traitement de données dépasse largement les frontières nationales et exige des réponses internationales pour garantir le respect des droits et libertés fondamentales, notamment le droit à la vie privée.

Dans cette optique, et sans pour autant changer aux fondements de la loi, notamment son approche technologiquement neutre, nous sommes d'avis que certains aménagements sont nécessaires d'une part, pour harmoniser notre législation avec le droit européen et pouvoir ainsi mieux répondre aux attentes des entreprises actives sur le plan international, d'autre part, pour répondre aux nouveaux défis technologiques. En particulier, il conviendrait d'assurer une plus grande transparence des traitements de données personnelles, de renforcer les obligations et les responsabilités de ceux qui traitent des données, de garantir la maîtrise des individus sur leurs données et de renforcer l'effectivité de la loi.

Nous estimons également nécessaire d'étendre le champ d'application de la loi à l'ensemble des traitements effectués par des organes fédéraux et d'aligner les définitions sur celles du droit européen. En outre, la distinction entre les secteurs public et privé s'amoindrit et on est en droit de s'interroger sur l'opportunité de les soumettre à des régimes de protection des données différents.

Il serait à notre avis également nécessaire de compléter et de préciser les principes de base de la protection des données. Ainsi, le principe de proportionnalité devrait être complété par le principe de minimisation des données. Il convient en effet d'éviter que des données personnelles soient collectées et traitées sous une forme identifiant la personne lorsque cela n'est pas nécessaire à la finalité du traitement. L'offre de services anonymes ou permettant l'usage de pseudonymes devrait être encouragé. Il faudrait favoriser la création de systèmes de gestion des identités conforme à la protection des données (la gestion de l'identité devrait se baser sur le recours à des procédures anonymes ou sous pseudonymes et la conservation décentralisée des données d'identification se baser sur un contrôle aussi large que possible par la personne concernée). La transparence des traitements devrait par ailleurs être renforcée, notamment en étendant l'obligation d'information pour toute collecte de données, indépendamment de leur nature, et en étendant le catalogue des informations à fournir en particulier lors d'activités de profilage.

De plus en plus de décisions ou de mesures affectant les personnes sont aujourd'hui le fruit de procédures automatisées pour lesquelles l'intervention humaine est relativement limitée. À l'instar de l'ensemble des législations européennes, la LPD devrait être complétée par des dispositions régissant le recours à des décisions automatisées.

La complexité des traitements de données, l'opacité qui les entourent, notamment lors d'opérations sur Internet, la dispersion des informations au travers du nuage électronique ou la multiplication des acteurs ayant accès à l'information affaiblit la position des personnes concernées, leur possibilité de faire valoir leurs droits et l'effectivité de la protection des données. Il convient dès lors de s'interroger sur les moyens d'améliorer la confiance des personnes dans les systèmes de traitement des données les concernant. Nous estimons ainsi nécessaire de renforcer la responsabilité de ceux qui traitent des données personnelles ou qui développent des systèmes de traitement et des produits. Il devrait être obligatoire de prendre en compte les principes de la protection des données dans l'organisation (notamment évaluation de risques, étude d'impact sur la vie privée, définition des processus de traitement, audit de protection des données, concept de protection des données contraignant, publication des politiques de vie privée et des procédure de traitements internes de plaintes) et dans le développement des systèmes d'information («protection des données par défaut») afin d'éviter la collecte et le traitement de données superflues et afin d'offrir aux personnes une meilleure maîtrise sur leurs données personnelles. Les obligations des responsables de traitement pourraient être complétées par l'introduction d'une obligation d'annoncer les brèches de sécurité des données, celle d'avoir un représentant en Suisse qui répond des exigences de protection des données dès lors que des activités de traitement y sont déployées, ou encore celle d'avoir un conseiller à la protection des données.

Pour améliorer l'effectivité de la loi et les possibilités de contrôle, nous préconisons de prévoir un contrôle préalable des traitements à risque (menace grave pour le droit à la protection des données), sous forme de notification préalable auprès du PFPDT et de renforcer le recours à la certification. La possibilité de recourir à une forme d'auto réglementation soumise à approbation de l'autorité (règles sectorielles contraignantes) pourrait également être envisagé. Parallèlement, les compétences du PFPDT pourraient être étendues et ses pouvoirs d'investigation renforcés (notamment droit de saisie, droit de consulter les données, droit de délivrer des sanctions pécuniaires). L'exercice des droits des personnes concernées devrait être également amélioré en facilitant l'accès à la justice (par exemple gratuité de la procédure), en introduisant un droit d'action des associations ou en étudiant d'autres mécanismes de résolution des conflits, comme la médiation.

L'un des grands défis de l'Internet et du monde virtuel a trait à la gestion et à la maîtrise des données. Une fois en ligne, l'information demeure et peut faire l'objet de

traitements multiples dans des contextes différents. Toutes les actions de l'internaute peuvent être répertoriées et tracées quelle que soit sa position: le développement fulgurant des téléphones intelligents accentue encore le phénomène. Il convient de réfléchir au moyen de garantir dans le monde virtuel les mêmes droits que dans le monde réel en affirmant en particulier le droit à l'oubli dans les réseaux et en se donnant les moyens de le garantir (date de péremption des données, obligation de désindexation, réglementation de la géolocalisation, droit de surfer sans être observé et profilé, droit de s'opposer à la publication ou l'indexation de données sur Internet, etc.).

D'autres éléments pourraient également être pris en considération dans l'optique d'une modernisation du droit à la protection des données comme un renforcement de la protection des données des mineurs, l'introduction du consentement pour le démarchage et la publicité en ligne, la responsabilité objective du fait du traitement, l'exercice des droits d'accès et de rectification en ligne.

Enfin, la lisibilité de la loi et son accessibilité y gagneraient si on regroupait dans un texte les dispositions générales et sectorielles régissant la protection des données et la transparence (code de la protection des données et de l'accès aux documents officiels).

3.2 Projet de migration du système de gestion des affaires du PFPDT

Nous planifions la migration vers un des produits GEVER standardisés. Dans ce but, nous nous concentrons en particulier sur les exigences organisationnelles, techniques et financières que cela implique.

Comme tous les offices fédéraux, nous travaillons à l'introduction d'un nouveau système GEVER pour remplacer notre actuel système de gestion des affaires (EDÖB-Office) qui assure depuis plus de dix ans la confidentialité de nos documents grâce à un chiffrement intégral des contenus sensibles et confidentiels.

Une telle migration requiert une intense planification organisationnelle, technique et financière. Nous avons ainsi entièrement redéfini notre plan de classement des dossiers (qui doit encore être approuvé par les Archives fédérales suisses) et avons réactualisé nos prescriptions organisationnelles de travail. En parallèle, nous nous sommes fait démontrer les deux produits standardisés, et avons en particulier examiné leur aptitude à garantir une haute confidentialité des données. Il en ressort clairement qu'aucun des produits proposés n'offre une confidentialité comparable à celle que nous connaissons depuis plus d'une décennie, raison pour laquelle nous avons différé notre choix. Raisons budgétaires en sus, la planification de la formation des utilisateurs avant la migration GEVER proprement dite s'en trouve ainsi légèrement retardée.

Dans le contexte de ce projet, nous avons dès lors porté nos efforts sur la définition des exigences techniques minimales qu'un système GEVER doit remplir en matière de protection des données et de transparence administrative (cf. ch. 1.2.11 du présent rapport d'activités).

3.3 5e Journée européenne de la protection des données – campagne pour les enfants

La sensibilisation des enfants et des adolescents a été, cette année également, un de nos chantiers majeurs au niveau de la formation. C'est dans ce cadre que nous avons, en partenariat avec le Conseil pour la protection de la sphère privée, lancé la campagne multimédia «NetLa – mes données m'appartiennent!». Celle-ci familiarise les enfants et adolescents de 5 à 14 ans avec l'importance de la personnalité et de la protection de la personnalité. La campagne a été présentée au public à l'occasion de la 5e journée européenne de la protection des données.

De nos jours, les enfants utilisent Internet souvent déjà dès l'âge préscolaire, sans être conscients des risques que cela comporte. Ils révèlent facilement des informations, s'enregistrer auprès de réseaux sociaux et publient par exemple leurs propres photos. L'objectif de NetLa est sensibiliser les enfants et les adolescents à un usage responsable des données personnelles sur Internet.

La plateforme centrale de cette campagne qui a été lancée le 28 janvier 2011, lors d'une conférence de presse dans le cadre de la 5e journée européenne de la protection des données est le site web www.netla.ch. Celui-ci propose des bandes dessinées et des jeux en ligne pour trois tranches d'âge (âge préscolaire, 7-10 ans et 11-14 ans). Dans la rubrique «Conseils et trucs», les parents peuvent s'informer sur les risques que courent leurs enfants lorsqu'ils utilisent les médias numériques et sur les mesures de protection qu'ils peuvent prendre. Pour l'enseignement, NetLa offre un matériel pédagogique qui permet d'aborder le sujet de la protection de la personnalité et des données.

3.4 Matériel pédagogique sur la protection des données destiné aux jeunes

Dans le but de sensibiliser les jeunes à un usage responsable de leurs données personnelles, nous avons développé un matériel pédagogique qui peut être utilisé par les enseignants depuis juillet 2010. Une attention particulière a été portée aux risques liés à l'utilisation des médias numériques.

Les jeunes grandissent au milieu des appareils et applications des technologies de l'information et des communications, et les utilisent de manière ludique et tout à fait naturelle. Ainsi ils «chattent» avec des personnes dont ils ont fait connaissance sur Internet, mettent des photos d'eux-mêmes ou de leurs amis dans leurs profils de réseaux sociaux ou s'enregistrent à des jeux en ligne avec leurs données personnelles. Souvent, Internet sert également à régler des conflits avec la différence que les insultes, accusations et diffamations sont, contrairement à la cour de récréation, accessibles à un public dans le monde entier.

Ce comportement naturel avec le téléphone mobile et l'ordinateur présente des risques: une fois que les données personnelles sont sur Internet, des millions de personnes peuvent en théorie y accéder et les utiliser à des fins qui portent atteinte à la personnalité des personnes concernées (p. ex. harcèlement, diffamation, vol d'identité, stalking ou pédophilie). Avec le matériel pédagogique pour jeunes de 15 à 18 ans que nous avons développé avec l'agence Kik, les enseignants disposent d'une bonne base de travail pour aborder en classe le thème de la protection des données et de la personnalité. Il comprend dix leçons indépendantes les unes des autres, qui permettent aux écoliers et écolières de réfléchir de manière active sur les rapports qu'ils ont avec leur vie privée, leurs données et les risques que comportent les médias numériques. Y sont abordés non seulement les perfidies des réseaux sociaux tels que Facebook et myspace, mais aussi l'importance d'utiliser des mots de passe sûrs ou les traces que nous laissons inconsciemment derrière nous lors de nos séances sur la Toile.

Ce matériel pédagogique, disponible en français, allemand et italien, peut être téléchargé gratuitement par toute personne intéressée sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet – Enfants et adolescents.

3.5 Publications du PFPDT – Nouvelles parutions

Nous publions sur notre site web des informations relatives à nos activités dans les domaines de la protection des données et du principe de la transparence. Parmi les contenus qui ont nouvellement été ajoutés figurent notamment les explications concernant les compteurs électriques numériques (compteurs intelligents), une vue d'ensemble des situations possibles lors de l'externalisation de traitements de données à l'étranger ainsi qu'une brochure de bandes dessinées qui rappelle les risques liés à l'utilisation des médias numériques.

Avec la nouvelle loi sur l'approvisionnement en électricité, le marché de l'électricité connaît une dérégulation progressive depuis le 1er janvier 2008. Cette ouverture du marché entraîne une séparation entre le réseau et l'énergie fournie. Pour planifier l'approvisionnement en électricité et l'offre de tarifs avantageux, les fournisseurs d'énergie ont besoin d'informations précises sur la consommation d'électricité, qui doivent être fournies par des compteurs d'énergie numériques, appelés «compteurs intelligents». Nos explications à ce sujet examinent les risques d'une mesure numérique de la consommation pour la sphère privée des consommateurs et présentent les mesures qui doivent être prises pour assurer une exploitation de ces compteurs qui soit conforme aux exigences de la protection des données (cf. ch. 1.8.1 du présent rapport d'activités). Ces informations se trouvent sur le site www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Autres thèmes.

Concernant le thème de l'externalisation, nous avons rédigé des explications qui analysent les diverses situations qui peuvent se présenter lorsque des traitements de données sont confiés à des acteurs à l'étranger et qui énumèrent les exigences sur le plan légal. En vertu de la loi sur la protection des données, le mandant doit conclure avec le mandataire un contrat qui règle les modalités du traitement et de la communication des données par ce dernier. Nous avons modifié le contrat-type de manière à ce qu'il tienne compte de la modification décidée en février 2010 par la Commission européenne des dispositions contractuelles standard relatives à ce domaine. Les deux documents se trouvent sous la rubrique Thèmes – Protection des données – Transmission à l'étranger (voir aussi chiffre 1.8.2 du présent rapport d'activités).

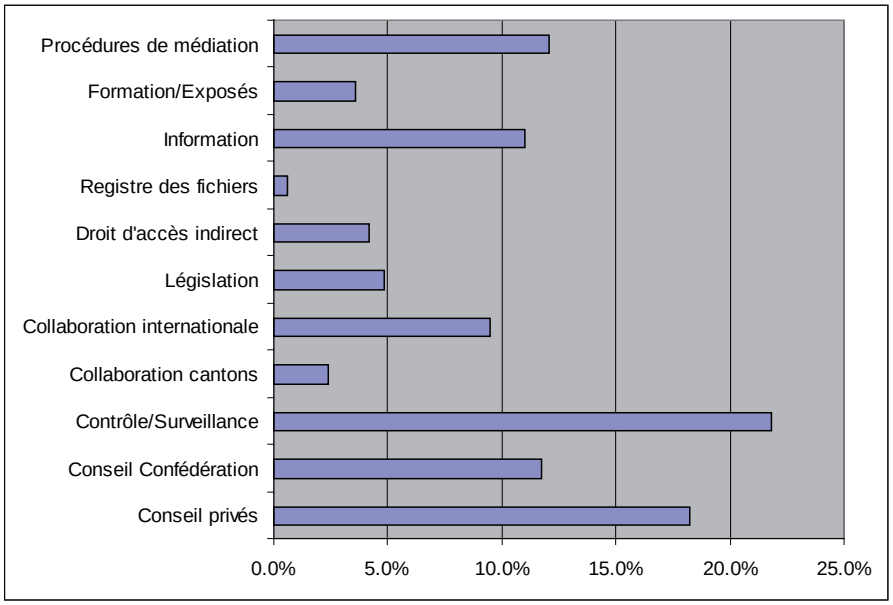
Dans le but d'augmenter la sécurité et la confiance de la population dans l'utilisation des technologies de l'information et de la communication (TIC), divers organismes de la Confédération et des cantons, dont le PFPDT, ont publié la brochure «Petites histoires d'Internet – que personne ne voudrait vivre». Elle contient des histoires qui présentent des situations dangereuses sur le web et fournissent des conseils sur la manière de les éviter, p. ex. en montrant qu'il vaut la peine de protéger de manière adéquate l'accès

au PC, au réseau sans fil et aux applications personnelles, ou que des images et messages mis sur la Toile en toute légèreté peuvent avoir des conséquences fâcheuses, p. ex. lors d'une candidature. Les histoires sont complétées par des liens vers des informations plus détaillées des services spécialisés compétents. La brochure est disponible dans les quatre langues nationales ainsi qu'en anglais et peut être téléchargée gratuitement sur le site www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet. Elle peut également être commandée dans sa version imprimée sur le site www.geschichtenausdeminternet.ch.

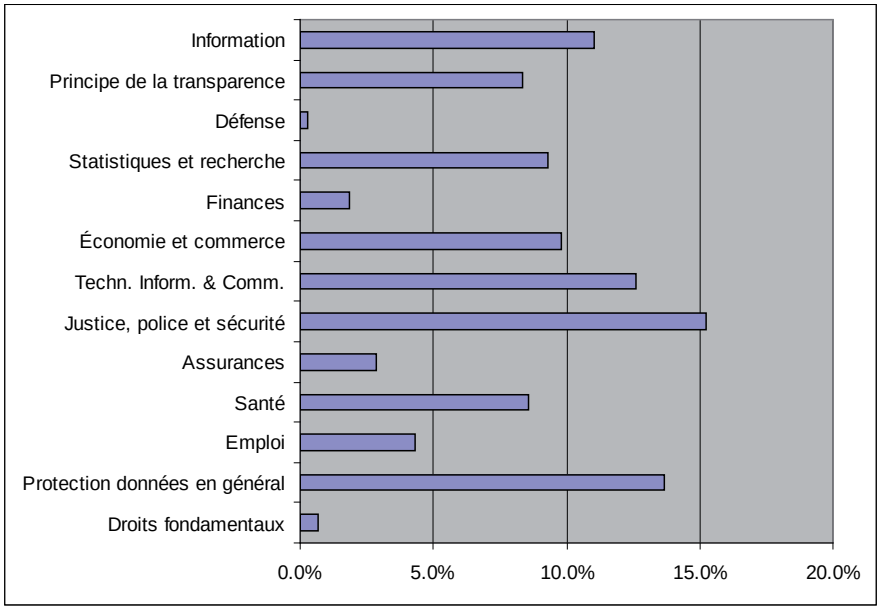
Nous avons également préparé un matériel pédagogique sur la protection des données destiné aux adolescents de 15 à 19 ans. Il est à disposition des enseignants pour aborder ce thème en classe. Les leçons mettent un accent particulier sur les médias numériques (voir aussi chiffre 3.4 du présent rapport d'activités ou sur notre site web www.leprepose.ch, sous la rubrique Thèmes – Protection des données – Internet – Enfants et adolescents).

3.6 Statistique des activités du Préposé fédéral à la protection des données et à la transparence (Période du 1er avril 2010 au 31 mars 2011)

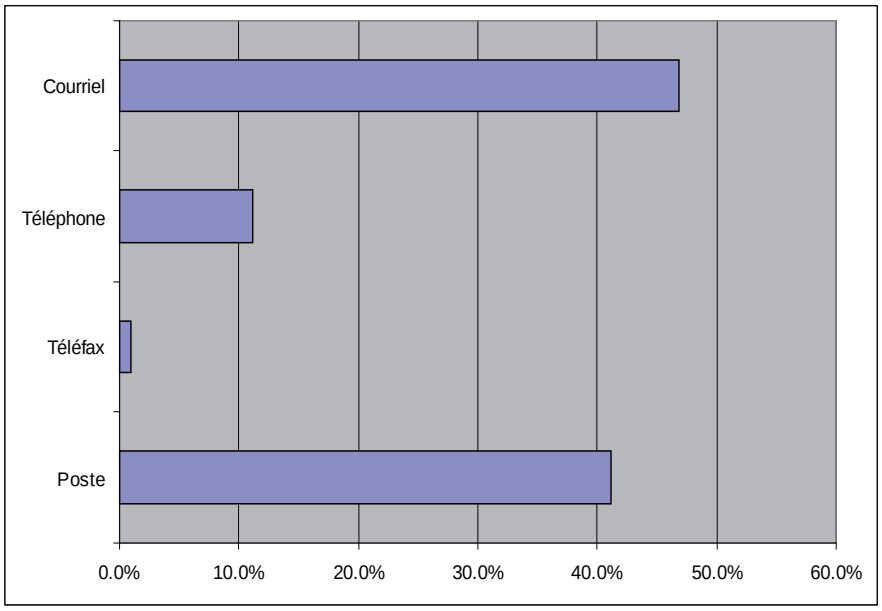
Charge de travail par tâches



Charge de travail par domaines



Provenance des demandes



3.7 Statistique des demandes d'accès présentées auprès des départements en vertu de l'art. 6 de la loi sur la transparence (Période du 1er janvier 2010 au 31 décembre 2010)

Dép.	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment / différé	Demande d'accès pendante
ChF	15	11	2	2	0
DFAE	39	18	6	15	0
DFI	54	18	16	17	3
DFJP	23	10	10	3	0
DDPS	8	5	2	0	1
DFF	17	6	4	5	2
DFE	31	13	10	7	1
DETEC	52	25	12	14	1
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%)	-
Total 2006 (en %)	95 (100%)	51 (54%)	41 (43%)	3 (3%)	-

Chancellerie fédérale ChF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante
ChF	5	2	2	1	0
PFPDT	10	9	0	1	0
TOTAL	**15**	**11**	**2**	**2**	**0**

Département fédéral des affaires étrangères DFAE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante
DFAE	39	18	6	15	0
TOTAL	**39**	**18**	**6**	**15**	**0**

Département fédéral de l'intérieur DFI

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment / différé	Demande d'accès pendante
SG DFI	4	1	2	1	0
BFEG	0	0	0	0	0
OFC	3	0	3	0	0
AFS	2	2	0	0	0
Météo Suisse	0	0	0	0	0
OFSP	32	9	6	14	3
OFS	1	1	0	0	0
OFAS	7	2	3	2	0
SER	0	0	0	0	0
Conseil des EPF	1	0	1	0	0
SWISS MEDIC	3	2	1	0	0
FNS	1	1	0	0	0
SUVA	0	0	0	0	0
TOTAL	**54**	**18**	**16**	**17**	**3**

Département fédéral de justice et police DFJP

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment / différé	Demande d'accès pendante
SG DFJP	0	0	0	0	0
OFJ	3	1	2	0	0
FEDPOL	3	2	1	0	0
METAS	0	0	0	0	0
ODM	8	4	3	1	0
MPC	3	0	3	0	0
ISDC	0	0	0	0	0
IPI	2	2	0	0	0
CFMJ	3	1	0	2	0
CAF	1	0	1	0	0
ASR	0	0	0	0	0
CSI	0	0	0	0	0
CNPT	0	0	0	0	0
TOTAL	**23**	**10**	**10**	**3**	**0**

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

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante
SG DDPS / BIG	7	5	1	0	1
Défense/ armée	1	0	1	0	0
armasuisse	0	0	0	0	0
OFPP	0	0	0	0	0
OFSPO	0	0	0	0	0
TOTAL	**8**	**5**	**2**	**0**	**1**

Département fédéral des finances DFF

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante
SG DFF	2	1	0	1	0
AFF	1	1	0	0	0
OFPER	1	0	1	0	0
AFC	5	2	2	1	0
AFD	0	0	0	0	0
RFA	0	0	0	0	0
OFCL	1	0	0	1	0
OFIT	1	0	0	1	0
CDF	6	2	1	1	2
SFI	0	0	0	0	0
PUBLICA	0	0	0	0	0
CC	0	0	0	0	0
TOTAL	**17**	**6**	**4**	**5**	**2**

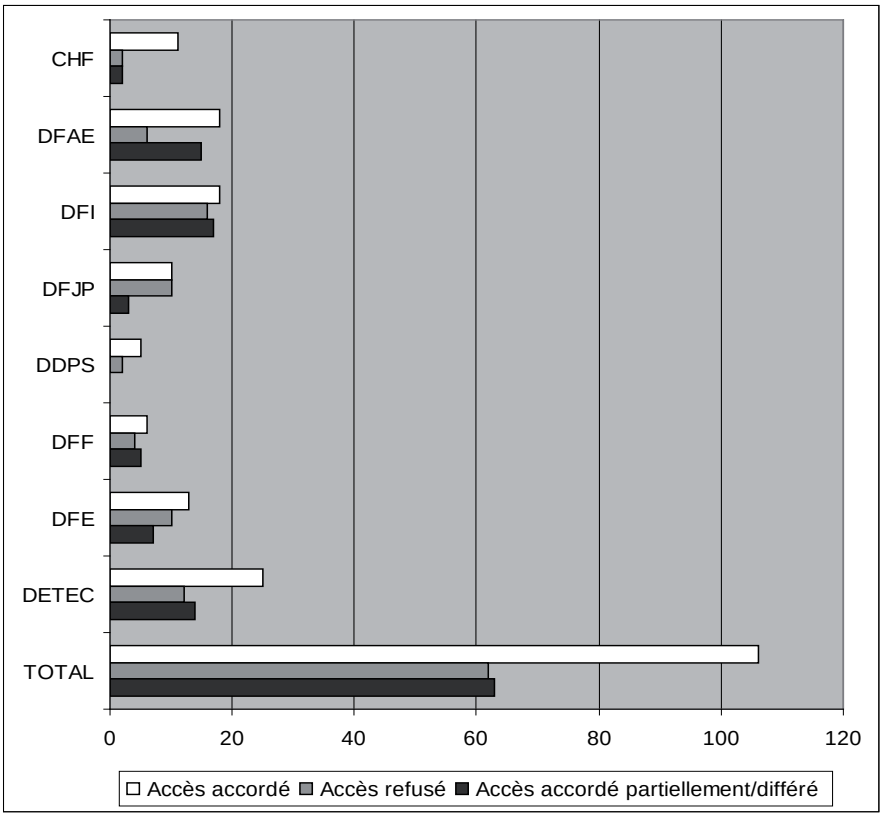
Département fédéral de l'économie DFE

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partielle-ment / différé	Demande d'accès pendante
SG DFE	1	1	0	0	0
SECO	7	2	2	2	1
OFFT	2	2	0	0	0
OFAG	14	4	5	5	0
OVF	3	2	1	0	0
OFAE	0	0	0	0	0
OFL	0	0	0	0	0
SPr	1	0	1	0	0
COMCO	2	1	1	0	0
ZIVI	0	0	0	0	0
BFC	1	1	0	0	0
TOTAL	**31**	**13**	**10**	**7**	**1**

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

Section concernée	Nombre de demandes d'accès	Accès accordé	Accès refusé	Accès accordé partiellement / différé	Demande d'accès pendante
SG DETEC	0	0	0	0	0
OFT	5	3	1	0	1
OFAC	10	2	6	2	0
OFEN	4	0	1	3	0
OFROU	3	3	0	0	0
OFCOM	6	2	1	3	0
OFEV	9	4	2	3	0
ARE	1	0	1	0	0
COMCOM	1	1	0	0	0
IFSN	6	4	0	2	0
PostReg	1	0	0	1	0
AIEP	6	6	0	0	0
TOTAL	**52**	**25**	**12**	**14**	**1**

Traitement des demandes d'accès



3.8 Statistique des demandes d'accès présentées auprès des Services du Parlement en vertu de l'art. 6 de la loi sur la transparence (Période du 1er janvier 2010 au 31 décembre 2010)

Services du Parlement

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

3.9 Nombre de demandes de médiation par catégories de requérants (Période du 1er janvier 2010 au 31 décembre 2010)

Catégorie de requérants	2010
Médias	17
Personnes privées (ou requérants ne pouvant pas être attribués de manière précise)	5
Représentants de milieux intéressés (associations, organisations, sociétés, etc.)	6
Entreprises	1
Avocats	3
Universités	0
Total	**32**

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

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

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

Secrétariat:

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

4. Annexes

4.1 Protection des données

4.1.1 Explications concernant l'utilisation des compteurs électrique intelligents

En vertu de la nouvelle loi sur l'approvisionnement en électricité, le marché de l'électricité connaît une dérégulation progressive depuis le 1er janvier 2008. Alliée à l'arrivée sur le marché de divers agents énergétiques de substitution, cette évolution requiert une nouvelle technique de mesure de la consommation. Les compteurs numériques, appelés «compteurs intelligents», peuvent mémoriser de très grandes quantités de données, ce qui recèle des risques pour la sphère privée.

Ci-après nous passons en revue les principaux risques en matière de protection des données auxquels s'expose l'utilisateur de compteurs intelligents et formulons des recommandations à ce sujet.

Libéralisation du marché de l'électricité et énergies renouvelables

La nouvelle loi sur l'approvisionnement en électricité est entrée en vigueur le 1er janvier 2008. Elle prévoit l'ouverture progressive du marché régulé par l'État. Dans une première étape, seuls les grands consommateurs, qui consomment annuellement plus de 100 MWh, ont libre accès au marché. Quelque 50'000 entreprises peuvent choisir librement leur fournisseur d'électricité depuis 2009, ce qui a constitué un changement majeur pour les quelque 900 entreprises d'approvisionnement en électricité en Suisse. Dans une seconde étape, les petites entreprises et les ménages pourront eux aussi, dès 2014, accéder librement au marché. De ce fait, les clients en Suisse pourront à l'avenir décider librement auprès de quel fournisseur ils souhaitent s'approvisionner en électricité. Cela dit, cette deuxième étape sera – comme la première – sujette au référendum facultatif.

Cette ouverture du marché entraînera la séparation entre le réseau et l'énergie fournie. En d'autres termes, le client aura à l'avenir un exploitant de réseau et un fournisseur d'électricité; le premier lui sera imposé, mais il pourra choisir le second.

En outre, la part croissante d'électricité issue d'agents énergétiques de substitution (énergie solaire ou éolienne) dans le réseau nécessite une meilleure gestion du courant injecté et de la consommation d'énergie. À la différence de l'électricité d'origine solaire ou éolienne, l'électricité provenant de centrales traditionnelles (énergie nucléaire, charbon, pétrole, gaz) est relativement facile à gérer. La compensation des fluctuations de

charge s'effectue par réglage de la puissance de certaines de ces centrales, par l'utilisation de centrales hydrauliques (centrales à accumulation avec pompage) et par le commerce d'électricité.

Pour planifier l'approvisionnement en électricité et l'offre de tarifs avantageux, il faut des pronostics de consommation précis, car les surcapacités et les sous-capapacités imprévues sont onéreuses pour les fournisseurs. A cet effet, ces derniers ont besoin d'informations détaillées sur la consommation d'énergie des ménages. Afin d'assurer une exploitation du réseau plus régulière et plus efficace, on pourrait même imaginer de piloter des appareils ménagers gros consommateurs d'électricité en fonction du taux d'utilisation du réseau. On pourrait par exemple reporter les intervalles de refroidissement des réfrigérateurs et des congélateurs ou le rechargement des batteries des véhicules sur des périodes de faible utilisation du réseau.

Compteurs classiques et compteurs numériques

Jusqu'à présent, la consommation d'énergie était enregistrée à l'aide de compteurs électromécaniques à simple tarif ou à double tarif. Le compteur à simple tarif a un seul dispositif de comptage et enregistre la consommation totale d'électricité. Lorsque l'usine électrique fournit du courant au tarif heures pleines et au tarif heures creuses, on utilise des compteurs à double tarif, qui enregistrent séparément la consommation d'électricité au tarif heures pleines (principalement de jour) et au tarif heures creuses. La lecture des compteurs s'effectue sur place, une ou deux fois par année.

Du fait de la séparation entre exploitant de réseau et fournisseur d'énergie, il faut que les compteurs puissent être commutés individuellement puisque les différents fournisseurs axent leurs tarifs sur l'offre et la demande. Pour ce faire, les compteurs numériques doivent pouvoir enregistrer la consommation d'énergie à intervalles variables. Les compteurs numériques permettent par ailleurs le pilotage à distance, ce qui signifie qu'ils peuvent être lus à n'importe quel moment, sans qu'une personne doive se déplacer. Ils pourront donc être relevés de manière plus souple et plus avantageuse.

Mais ces compteurs offriront encore d'autres possibilités: le client pourra, selon l'exploitant et le fournisseur, accéder via Internet ou un écran d'affichage dans son logement à ses données de consommation en temps réel ou à l'historique de ses données. Cela devrait l'inciter à réduire sa consommation d'énergie.

Risques du point de vue de la protection des données

Les compteurs intelligents peuvent indiquer la consommation d'énergie totale et la consommation d'énergie en temps réel ainsi que l'heure à laquelle l'énergie est utilisée. Selon la configuration de l'appareil, les profils de charge d'un ménage seront plus

ou moins détaillés. Pour établir un tel profil, le compteur enregistre tous les quarts d'heure la consommation d'énergie (35'000 points de mesure par an) et mémorise ces informations jusqu'à ce qu'il soit relevé ou que d'autres données viennent se surimprimer sur les anciennes.

Du fait de leur conception technique, les compteurs numériques permettent en principe d'enregistrer les données nécessaires à la facturation, mais aussi le profil de consommation d'énergie du ménage ou de l'entreprise. Ces données plus détaillées contiennent des informations qui peuvent s'avérer précieuses pour le client en lui indiquant sa consommation d'énergie et donc aussi des gisements d'économies d'énergie, mais elles recèlent aussi des informations sur ses activités professionnelles, ses processus de production, ses activités personnelles, l'organisation de ses journées, des absences maladie, etc. De l'avis du préposé fédéral à la protection des données (préposé), il n'est toutefois pas nécessaire que ces informations détaillées soient automatiquement transmises au fournisseur d'énergie ni à l'exploitant de réseau. Des pronostics concernant les besoins en énergie peuvent aussi être établis sur la base de données rendues anonymes et provenant de plusieurs ménages regroupés.

Mesures à prendre

Lors de la collecte de données non indispensables à la facturation, soit lors de l'établissement du profil de charge détaillé d'un ménage, les principes de la protection des données doivent être respectés. En d'autres termes, tant pour ce qui est de l'information des personnes concernées que s'agissant de la conception du système, les données doivent être traitées conformément au principe de la proportionnalité et dans le but indiqué lors de leur collecte, le traitement et sa finalité doivent être reconnaissables, et la sécurité des données doit être assurée. En rapport avec les réseaux intelligents («smart grids»), cela signifie concrètement qu'il faut respecter les points suivants:

Le principe de la proportionnalité exige qu'on ne récolte pas plus de données personnelles que ne l'exige le but du traitement. Le but du traitement doit être indiqué lors de la récolte des données, p. ex. dans les conditions générales de vente, et il ne doit pas être formulé de façon si générale qu'il puisse s'appliquer à tous les types de traitement. Il convient de fixer d'entrée de jeu dans quel but les données seront utilisées et de sélectionner les données indispensables à cet effet. Cela permet d'éviter qu'on collecte toutes sortes d'informations pour parer à toute éventualité.

La sécurité des données doit être assurée tout au long de la durée de vie des données, depuis le moment où elles sont générées par le compteur intelligent jusqu'à ce qu'elles soient effacées par le fournisseur d'énergie ou l'exploitant de réseau; ce principe vaut non seulement pour les méthodes classiques de relevé de l'énergie consommée et

l'enregistrement des données, mais aussi pour les différentes possibilités de transmission (écran d'affichage chez soi, transmission à l'exploitant de réseau / au fournisseur d'énergie).

Au cas où le traitement des données est confié à des tiers, il convient en outre de se conformer aux dispositions de l'art. 10a de la loi sur la protection des données (LPD).

Recommandations du préposé

- Informer de manière claire et détaillée les personnes concernées au sujet du traitement des données (dans quel but les données sont traitées, mais aussi si elles seront transmises à des tiers), p. ex. dans les conditions générales de vente.
- Pour établir des pronostics concernant les besoins, prélever des données rendues anonymes et regroupées à partir de plusieurs ménages au lieu d'établir des profils de charge détaillés pouvant être attribués à un ménage particulier.
- Les exploitants de réseau et les fournisseurs d'énergie ne doivent pas avoir accès aux données en temps réel.
- Contrôle d'accès et journalisation des relevés des compteurs mesurant la consommation d'énergie/le profil de charge.
- Contrôle d'accès et journalisation en cas de mémorisation des profils de charge auprès des fournisseurs d'énergie et des exploitants de réseau.
- Crypter les données transmises à l'intérieur du bâtiment ou aux fournisseurs d'énergie et aux exploitants de réseau.
- Protéger les données contre la perte, le vol, l'accès non autorisé, la communication, l'utilisation ou la modification.
- Demander le consentement des personnes concernées avant de transmettre ou d'exploiter des profils de charge se rapportant à des ménages.

Informations complémentaires

Des recommandations pour la mise en oeuvre des compteurs électriques «intelligents» (CNIL)

http://www.cnil.fr/la-cnil/actu-cnil/article/article/des-recommandations-pour-la-mise-en-oeuvre-des-compteurs-electriques-intelligents/

The Smart Grid and Privacy, Electronic Privacy Information Center

http://epic.org/privacy/smartgrid/smartgrid.html

4.1.2 Recommandation concernant «L'utilisation de données biométriques pour le système de réservation du club de tennis XX»

Utilisation de données biométriques

pour le système de réservation

du club de tennis XX

Rapport final

du 13 septembre 2010

du contrôle
du Préposé fédéral à la protection des données
et à la transparence (PFPDT)
selon art. 29 de la loi fédérale
sur la protection des données (LPD)

1. Point de départ

Le club de tennis XX a introduit en été 2009 un nouveau système pour la réservation des courts de tennis. Les empreintes digitales des membres sont dès lors saisies et enregistrées sous forme de gabarits biométriques. Chaque réservation d'un court de tennis doit désormais être confirmée par le numéro de membre et surtout par l'apposition de l'empreinte digitale, afin de pouvoir jouer sur le court correspondant.

Le nouveau système de réservation vise à garantir que seules les personnes autorisées puissent utiliser les courts du CT XX.

2. Portée du contrôle

Le contrôle de protection des données portait sur les flux de données en rapport avec le nouveau système de réservation. Le point principal résidait dans le traitement des données biométriques collectées, ainsi que des données personnelles publiées dans le cadre de la réservation en ligne.

3. Chronologie du contrôle

Début octobre 2009	Le PFPDT apprend l'existence du système biométrique de réservation par le biais de demandes de membres du club. Suite au développement d'une certaine résistance au sein du club et au nombre important (plus de 1000) de personnes concernées, le PFPDT décide de procéder à un établissement des faits.
15.10.2009	Le PFPDT informe le CT XX par écrit sur le contrôle de protection des données envisagé pour le système de réservation et sur l'établissement des faits prévu sur place. En outre, le PFPDT demande une documentation au sujet du nouveau système et des réponses à un formulaire de questions annexées.
30.10.2009	Le CT XX répond au formulaire de questions et envoie une première documentation.
03.12.2009	Le PFPDT pose quelques questions complémentaires.
14.12.2009	Le CT XX répond à ces nouvelles questions et envoie d'autres documents.
14.01.2010	Le PFPDT propose des dates de visite et demande quelles seront les personnes présentes.
27.01.2010	Le rendez-vous est fixé au 11.02.2010.
11.02.2010	Établissement des faits en présence des personnes responsables.
fin février 2010	Échange de courriels entre le PFPDT et le CT XX au sujet de questions complémentaires.
05.03.2010	Le PFPDT envoie un factsheet au CT XX en les priant de vérifier matériellement le texte et de répondre aux questions supplémentaires.
22.03.2010	Le CT XX confirme par écrit l'exactiture du contenu du factsheet.
Avril 2010	Analyse et synthèse de tous les documents et états de fait, ainsi que préparation du rapport final par le PFPDT.
13.09.2010	Envoi au CT XX du rapport final de contrôle du PFPDT.

4. Établissement des faits du 11 février 2010

4.1 Personnes présentes

- Président du CT XX
- Avocat-conseil du CT XX
- Consultant système du CT XX
- 2 représentants du fournisseur du système
- 2 collaborateurs du PFPDT

4.2 Enrôlement biométrique

L'enrôlement est accompli de manière autonome par chaque membre. Les informations personnelles ainsi que le numéro d'adhérent figurent déjà dans la base des données des membres du club. L'adhérent introduit son numéro de membre sur le pavé numérique et présente son doigt sur le lecteur d'empreintes digitales. Le gabarit extrait de cette numérisation, comportant une douzaine de minuties, est mémorisé dans l'ordinateur local «PC biométrique» sous le numéro correspondant de membre et dans le format livré par le lecteur. Nous pensons qu'il s'agit plus d'un codage que d'un chiffrement et ne disposons en tous les cas d'aucune information probante (algorithme, clé, longueur) quant à un éventuel chiffrement.

Le système de réservations fonctionne sans cartes, de sorte que toutes les données sont mémorisées de manière centralisée. Les gabarits ne se trouvent cependant pas sur le même ordinateur que les autres données concernant les membres. Ces dernières se trouvent sur un PC au secrétariat (base de données des membres) et sur un serveur Web (données de réservation). Le PC biométrique est cependant relié par réseau sans fil (WLAN/WPA) au PC du secrétariat, qui est lui-même connecté à Internet (ligne ADSL). Les données brutes des empreintes digitales ne sont pas du tout conservées. Selon les dires du fournisseur de lecteurs biométriques, il n'est en outre pas possible de reconstruire les données brutes à partir des gabarits mémorisés.

4.3 Réservation d'un court de tennis

Avant de pouvoir jouer sur un court, il faut impérativement le réserver. Cette opération peut avoir lieu directement sur place ou alors préalablement depuis internet. La réservation doit ensuite être confirmée au moyen de son empreinte digitale jusqu'à 10 minutes après le début de la rencontre. Tous les joueurs, à l'exception des invités, doivent confirmer leur participation avec leur empreinte digitale.

Pour ce faire, chaque joueur introduit son numéro de membre, avant d'être prié de présenter son doigt sur le lecteur biométrique. Le numéro de membre permet de retrouver automatiquement le gabarit de référence correspondant et de le comparer ensuite au gabarit présenté. Il s'agit donc bien d'une comparaison biométrique 1-1 (vérification) et non pas d'une comparaison 1-n (identification) avec toutes les références contenues dans la base de données. La réservation est confirmée si tous les joueurs inscrits réussissent leur vérification biométrique ou simplement annulée dans le cas contraire. Dans ce dernier cas, le court apparaît alors comme «libre» dans le système et peut à nouveau être réservé. Les joueurs peuvent être expulsés d'un court, si celui-ci n'est pas dûment marqué comme «réservé».

Le système de réservation (serveur Web) produit des fichiers journaux sur les réservations, qui sont elles-mêmes bien sûr enregistrées. Il est ainsi possible de consulter les réservations effectuées, soit l'utilisation des courts par les membres, de manière rétroactive pendant environ une année.

4.4 Effacement des données

Les données personnelles des membres sont mémorisées à trois endroits: dans les fichiers de gabarits (PC biométrique), dans la base de données des membres (PC secrétariat) et dans le système de réservation (serveur Web). Selon les affirmations de l'informaticien du club, toutes les données peuvent être détruites et ce à n'importe quel moment. Cependant, aucun délai de conservation ne serait pour l'instant prescrit, ceci étant dans le domaine de responsabilité du CT XX.

Lorsqu'un membre quitte le club, son gabarit peut simplement être détruit. Dans le système de réservation, les données principales sont détruites par les informaticiens tous les 2 à 3 ans et les fichiers journaux après environ 1 an, avant tout pour gagner de la place. L'administration du CT XX n'effectue elle-même aucun effacement régulier de données.

Le PFPDT a rendu attentif sur place au fait que le principe de proportionnalité des traitements de données impose un effacement aussi rapide que possible des données, et soulignons que le CT XX devrait introduire des règles pour un effacement approprié des données.

4.5 Devoir d'information et droit d'accès

Les membres ont été préalablement informés dans le cadre de la votation sur le système planifié lors de la dernière AG. Une discussion a eu lieu suite à cette assemblée, discussion au cours de laquelle d'autres informations ont été échangées. Après la décision d'introduire ce système, tous les membres ont en outre été informés au sujet de

ce système par poste, courriel et le magazine du club. Il n'existe par contre pas d'information standardisée pour les nouveaux membres. Le président s'engage à améliorer l'information aux membres, sur requête du PFPDT.

Les membres peuvent en tout temps s'adresser au président du club pour consulter leur gabarit. Sur proposition du PFPDT, le président s'est engagé à étendre ce droit d'accès à la base de données des membres et au système de réservations.

4.6 Alternatives à la saisie biométrique

Le système permet d'effectuer une réservation à l'aide d'un code personnel (PIN) au lieu d'une empreinte digitale. Les personnes qui ne peuvent ou ne désirent pas utiliser le système biométrique ont ainsi la possibilité d'éviter ce système. Cette alternative est pour l'instant utilisée par une dizaine de personnes. Sur demande expresse du PFPDT, le président s'est déclaré d'accord, d'informer à l'avenir les membres de manière transparente sur cette voie alternative.

4.7 Avantages du système de reconnaissance biométrique

L'installation du CT XX se compose principalement des courts de tennis et du clubhouse avec vestiaires et restaurant. Une réception ou quelque chose de comparable n'existe pas. C'est pour cette raison qu'un contrôle automatisé des ayants droits doit avoir lieu.

Le système de réservations fonctionnait jusqu'à présent à l'aide de codes personnels. Le problème rencontré était que certains PINs ont été ébruités et ainsi utilisés par plusieurs personnes externes au club. Le système a donc dû être modifié, de façon à ce qu'une vérification univoque avec un coût aussi faible que possible (les moyens financiers du club seraient modestes selon les dires du président) soit introduite. La vérification à l'aide d'empreintes digitales offre ces possibilités, raison pour laquelle elle a été choisie. Le club a vécu depuis lors une croissance sensible du nombre des membres, et les courts sont néanmoins moins surchargés qu'auparavant. Cela laisse à penser, que les abus du système précédent étaient significatifs.

On s'est consciemment décidé pour un système sans cartes personnelles. Les cartes peuvent en effet facilement être oubliées ou perdues, ce qui d'une part augmente le risque d'abus et d'autre part crée un désagrément supplémentaire pour les membres. La majorité des membres salue la solution sans cartes, car celle-ci serait bien plus confortable («on a toujours ses doigts avec soi…»). Le système serait accepté par une large majorité des membres et on serait satisfait de cette solution.

4.8 Communication de données à des tiers (externes)

Aucune donnée biométrique n'est communiquée à des tiers. Aucun transfert de ces données n'a lieu vers le fournisseur de lecteur biométrique, le système n'étant pas relié à cette entreprise.

Le système de réservations (sans données biométriques) est par contre consultable sans aucune forme de mot de passe à partir du site du club. Chaque internaute peut ainsi voir, qui a réservé quel court à quel moment, et ce de manière rétroactive pendant 2 à 3 ans. Chaque membre du club peut certes demander à modifier son nom d'utilisateur lors de la création de son compte et définir ainsi un pseudonyme, en particulier pour ce type d'affichage, plutôt que son identité réelle. Par défaut, le système retient la première lettre du prénom suivie des 20 premières lettres de son patronyme.

4.9 Localisation des ordinateurs, sécurité des données

Les gabarits sont mémorisés sur un ordinateur (PC biométrique) qui se trouve dans une antichambre du clubhouse. Ce local est sécurisé avec une porte normale munie d'une simple serrure, dont les détenteurs de clé sont: le président, le resp. informatique, l'intendant et 2-3 autres personnes. Sur une tablette à l'extérieur du local, cette borne offre aux utilisateurs les périphériques suivants: un pavé numérique pour introduire le numéro d'adhérent, un lecteur d'empreintes digitales et une souris permettant de déplacer le curseur sur l'écran et de cliquer sur la fonction désirée.

Les données des membres se trouvent sur un PC dans le secrétariat du club, situé au premier étage du clubhouse et accessible de l'extérieur par une galerie. Le secrétariat est également fermé par une porte normale munie d'une simple serrure et peut être visité par n'importe qui durant les heures d'ouverture. En dehors de celles-ci, le secrétariat est accessible aux détenteurs de clé suivants: le président, le resp. informatique, l'intendant, 4 membres du comité et 4 professeurs employés par le club. L'accès logique au PC administratif du secrétariat est cependant protégé par mots de passe. Notons encore que ce PC administratif a accès aux gabarits par le biais d'un partage caché qui a été créé sur le PC biométrique. Pour augmenter la sécurité de cet accès, il a été suggéré de créer un profil particulier pour cette gestion.

Le système de réservations se trouve sur un serveur Web du fournisseur. L'accès aux données des personnes de la base de données est protégé par le mot de passe de l'administrateur du système. Nous ne connaissons par contre pas les conditions contractuelles de sécurité des données offertes par le fournisseur.

Les PC bénéficient tous deux d'un accès à Internet et ils communiquent entre eux par un réseau sans fils. Ce WLAN protégé pour l'instant par le protocole WPA (et dès mars 2010 par WPA2) peut être utilisé pour accéder à Internet aux alentours du clubhouse par tous les membres qui le désirent. Il leur suffit pour ce faire de demander le mot de passe d'accès.

Les données traditionnelles des membres sont enregistrées en texte clair, tandis que les gabarits sont mémorisés prétendument sous une forme chiffrée. Nous pensons cependant qu'il s'agit plus d'un codage (ASN.1 DER) que d'un chiffrement et ne disposons en tous les cas d'aucune information probante (algorithme, clé, longueur) quant à un éventuel chiffrement.

4.10 Maintenance du système

La maintenance du système est assurée par les informaticiens du CT XX. Grâce à leur codage/chiffrement, les gabarits ne peuvent pas être décodés dans le cadre des travaux de maintenance, à la différence des autres données mémorisées sous une forme claire.

5. Jugement du point de vue de la protection des données

5.1 Données biométriques en tant que données personnelles

5.1.1 Point de départ

La loi fédérale sur la protection des données du 19 juin 1992 (LPD; RS 235.1) est applicable dans chaque cas où des données personnelles au sens de l'art. 3 lit. a LPD sont traitées. Dans le cas présent, des données biométriques (gabarits d'empreintes digitales) sont traitées pour la réservation de courts de tennis.

5.1.2 Jugement du point de vue du PFPDT

Des données biométriques d'empreintes digitales sous forme de gabarits biométriques (données de référence) rendent une personne identifiable par comparaison avec une empreinte digitale présentée ultérieurement. Les données biométriques peuvent ainsi servir à authentifier/vérifier (resp. identifier) une personne. L'identifiabilité ne découle pas seulement de cette possibilité de comparaison biométrique, mais aussi par le fait qu'il existe une correspondance entre la base de données des gabarits (PC biométrique) et celle des membres (PC secrétariat). Par cette correspondance, les données biométriques sous forme de gabarits peuvent clairement être mises en relation avec une personne et la rendre ainsi identifiable (art. 3 lit.a LPD).

Dans le cas du CT XX, une douzaine de minuties extraites d'une empreinte digitale sont mémorisées. Les données de ces minuties sont en fait codées (et comprimées) au moyen d'un algorithme mathématique. Les algorithmes d'extraction de gabarits à partir de données biométriques brutes sont de nos jours ni standardisés, ni transparents. Il est de ce fait difficile de pouvoir évaluer formellement et définitivement la sensibilité (éléments sur la santé/race) d'un gabarit biométrique. De plus, les données biométriques brutes ou dérivées rendent une personne identifiée ou identifiable, tandis que leur collecte – en particulier celle des empreintes digitales – laisse en général des traces. La collecte de données biométriques brutes ou dérivées est ainsi susceptible de permettre la création d'un profil de mouvement de la personne concernée. En conséquence, il existe un potentiel élevé d'atteinte aux droits de la personnalité lors de la collecte de données biométriques. On doit par ailleurs constater, que le Conseil de l'Europe et le groupe de l'article 29 de l'UE (Directive 95/46/EC du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) reconnaissent pour les mêmes raisons le caractère sensible des données biométriques.

5.2 But du traitement de données

5.2.1 Point de départ

Chaque traitement de données personnelles peut entraîner une atteinte au droit à la protection de la sphère privée selon l'art. 13 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101). De ce fait, un tel traitement nécessite un motif justificatif particulier. Des considérations pratiques ou une simple convivialité pour les clients ne représentent essentiellement pas un motif justificatif suffisant pour le traitement de données biométriques.

Selon les indications du CT XX, la saisie des données biométriques n'a pour seul but, que d'empêcher les abus d'utilisation des courts de tennis par des personnes non autorisées. Avant l'introduction du système biométrique de réservation, les courts étaient réservés au moyen d'un NPI, ce qui s'est révélé être propice aux abus. Les codes ont été en partie transmis et utilisés par plusieurs personnes (non-membres). Ceci n'est plus possible avec le nouveau système biométrique. Le CT XX a par la suite aussi remarqué une hausse significative du nombre de membres, tandis que les courts étaient quant à eux moins fréquentés.

On a volontairement renoncé à l'utilisation de cartes individuelles de membre, car il y a le risque que les cartes soient perdues ou oubliées. C'est pour ces raisons de confort que les membres ont préféré un système biométrique sans carte.

5.2.2 Jugement du point de vue du PFPDT

Le nouveau système de réservation et la collecte conséquente de données biométriques poursuivent des finalités plausibles. Pour le PFPDT, on doit cependant se poser sérieusement la question de savoir s'il n'existe pas des alternatives pour éviter les abus qui porteraient moins atteinte aux droits de la personnalité des personnes concernées (cf. à ce sujet les remarques générales concernant la proportionnalité au chiffre 5.5).

5.3 Licéité du traitement de données / Consentement des personnes concernées

5.3.1 Point de départ

Les données biométriques sont des données personnelles au sens de la LPD, dont le traitement requiert un motif justificatif (art. 12 et 13 LPD). Dans le cas présent, le consentement des personnes concernées peut être retenu comme motif justificatif.

Selon les informations du CT XX, le système prévu a fait l'objet d'une discussion de principe lors d'une assemblée générale. Lors de la votation qui a suivi, la majorité des membres présents s'est prononcé en faveur de l'introduction d'un tel système biométrique. Le système a ensuite été introduit et une notice d'utilisation du système de réservation a été publiée sur le site resp. sur la «borne». Toujours selon les informations du CT XX, les nouveaux membres sont informés oralement par le président sur le système de réservation biométrique.

Il n'existe manifestement aucun enregistrement écrit concernant les informations remises aux membres lors de l'AG qui a ratifié l'introduction de ce système. On doit cependant partir de l'idée que les informations transmises n'étaient que de nature globale et ne renseignaient en particulier pas sur les modalités de traitement de données (par ex. nature et lieu de stockage des gabarits, durée de conservation, protection d'accès) dans le cadre du système biométrique de réservation.

La notice d'utilisation du système de réservation n'aborde que très superficiellement les modalités de traitement du système biométrique. Elle ne renseigne principalement que sur la procédure d'enrôlement et de réservation.

L'information orale du président a lieu à chaque fois de manière individuelle et n'est donc pas standardisée. On peut ici aussi partir de l'idée que le président n'informe pas au sujet des modalités de traitement.

D'autres supports d'information n'existent pas pour l'instant, mais ils devraient selon le CT XX être créés et remis aux membres du club.

Toutes les personnes qui ne peuvent ou ne veulent pas utiliser le système biométrique

de réservation, peuvent effectuer la réservation à l'aide d'un NPI comme jusqu'à présent. Jusqu'à présent, environ 10 personnes ont fait usage de cette possibilité. Les membres ne sont pas informés au préalable de cette alternative. L'alternative n'est proposée qu'au moment où quelqu'un refuse de saisir ses données biométriques ou s'il s'avère que le système biométrique est dans l'incapacité d'enrôler la personne concernée.

5.3.2 Jugement du point de vue du PFPDT

Du point de vue du PFPDT, le consentement de la personne concernée requiert des exigences sévères quant à sa mise au courant, en particulier dans un domaine aussi sensible que celui du traitement d'empreintes digitales. Il faut donc exiger que les membres soient informés plus concrètement sur les modalités de traitement, afin qu'ils soient au clair quant à la portée de leur consentement. Par conséquent, il faut communiquer aux personnes concernées les points essentiels du traitement de données, comme où et pour combien de temps les données biométriques sont mémorisées, que se passe-t-il avec les gabarits et les données de journalisation, qui possède les droits d'accès aux données et à qui ils peuvent, si jamais, être transférés. Tout cela devrait avoir lieu par le biais d'une feuille d'information standardisée qui devrait être distribuée à tous les membres existants ainsi qu'aux nouveaux. Cette feuille d'information doit être signée par l'administration et dotée d'un marquage de contrôle de version. Les membres doivent en outre être informés de l'existence de l'alternative (présentement la réservation par NPI), afin que le consentement ait lieu librement et pas sous la présupposition que l'on n'a pas le choix.

Les membres ne disposaient pas au moment de la votation de l'assemblée générale des connaissances nécessaires de l'état de faits leur permettant de donner un consentement juridiquement acceptable. De plus, on doit à ce stade encore préciser que seul le consentement individuel de chaque personne concernée peut justifier l'atteinte aux droits de la personnalité. Une décision majoritaire lors d'une AG ne remplit pas cette exigence.

On doit aussi partir de l'idée qu'à l'heure actuelle, les membres ne sont pas suffisamment informés sur les modalités de traitement pour pouvoir consentir valablement au traitement de données. Un consentement valable ne peut être vérifié qu'au moment où les exigences formulées ci-dessus sont remplies et les membres se décident pour le système biométrique de réservation en parfaite connaissance de ces informations.

5.4 Traitement selon la bonne foi / Transparence

5.4.1 Point de départ

Le traitement de données personnelles doit être effectué conformément au principe de la bonne foi (art. 4 al. 2 LPD). Cela signifie d'une part que le traitement doit être transparent pour la personne concernée et d'autre part que la collecte et chaque autre traitement de données doit être en principe reconnaissable pour la personne concernée.

Comme déjà mentionné au chiffre 5.3, les membres ont été informés après l'AG sur la collecte de données biométriques au moyen de la notice d'utilisation du système de réservation, ainsi qu'oralement par le président du club. Une feuille d'information standardisée n'existe cependant pas. L'enrôlement est effectué par le membre lui-même. Ce dernier doit donc agir activement pour que ses données biométriques puissent être saisies (glissement de son doigt sur le senseur biométrique de la «borne» près de l'entrée du clubhouse). Aucune donnée biométrique ne peut donc être collectée sans sa participation.

5.4.2 Jugement du point de vue du PFPDT

Comme les données biométriques ne peuvent être collectées sans participation de la personne concernée, le traitement de ces données a bien lieu d'une manière reconnaissable. Pour un traitement de données aussi transparent que possible, il faudrait remettre aux membres, en plus des informations actuellement communiquées oralement, une feuille d'information standardisée sur laquelle est décrit tout ce qui passe avec les données personnelles. Cette feuille peut se référer à ce qui est écrit au chiffre 5.3.

5.5 Proportionnalité du traitement de données

Le traitement de données personnelles doit être effectué conformément au principe de la proportionnalité (art. 4 al. 2 LPD). Cela signifie que celui qui traite des données ne peut traiter que celles dont il a effectivement objectivement besoin pour un but déterminé et qui sont en relation raisonnable avec la finalité du traitement et avec l'atteinte à la personnalité.

5.5.1 Proportionnalité matérielle – Point de départ

Un traitement de données n'est proportionnel que s'il se limite au contenu absolument nécessaire pour atteindre le but fixé. La proportionnalité matérielle demande de ménager le plus possible l'utilisation de données personnelles. Cela impose aussi qu'aucune

donnée excédentaire non indispensable au but poursuivi ne soit produite. Il est également irrecevable de collecter de manière provisionnelle des données personnelles, à moins que le but poursuivi ne l'exige impérativement.

Avec l'introduction du nouveau système de réservation, des gabarits biométriques sont générés à partir des empreintes digitales des membres, puis stockés dans une base de données centralisée. Les données biométriques brutes (i.e. l'image originale de l'empreinte digitale) ne sont pas conservées. Le système fonctionne sans cartes individuelles. Une réservation préalable d'un court à partir du système de réservation en ligne ou de la «borne biométrique» est confirmée par la saisie du numéro de membre suivie de l'apposition du doigt sur le lecteur biométrique. Le gabarit extrait du doigt présenté est comparé avec le gabarit de référence correspondant au numéro de membre introduit. Si les deux gabarits concordent, la réservation est confirmée et reste mémorisée et consultable dans le système de réservation pour les 2-3 prochaines années. Si les deux gabarits ne concordent par contre pas, la réservation n'est alors pas confirmée et radiée 10 minutes après le début de la période de réservation.

À côté des gabarits biométriques, d'autres données sur les membres (renseignements personnels, données sur les joueurs, etc.) sont conservées dans le PC du secrétariat et les données de réservation bien sûr dans le système der réservation. Les données de réservation sont consultables sans mot de passe sur Internet par n'importe quel internaute. Le nom d'utilisateur (par défaut la première lettre du prénom suivie au maximum des 12 premières lettres du nom de famille) et les périodes de réservation sont consultables pour les 2-3 années passées. Pour effectuer une réservation en ligne, le membre doit se connecter à l'aide de son nom d'utilisateur et de son mot de passe. Le nom affiché peut être modifié par le membre lui-même lors de son inscription.

5.5.2 Jugement de la proportionnalité matérielle du point de vue du PFPDT

5.5.2.1 Centralisation des données biométriques

La mise en œuvre de processus biométriques dans le domaine privé représente en fonction de leur conception dans le cas concret une atteinte plus ou moins intensive aux droits de la personnalité des personnes concernées. Avant la mise en œuvre de tels processus biométriques, il faut donc en principe toujours vérifier si d'autres mesures appropriées, mais moins attentatoires aux droits fondamentaux des personnes concernées, ne permettraient pas également d'atteindre le but visé. Par ailleurs, il faut déjà lors du choix et de la conception du processus biométrique veiller à choisir un système qui soit le plus économique possible en données et qui reste dans un rapport raisonnable avec le but visé. Comme le Groupe de l'art. 29 de l'UE le stipule dans sa prise de position sur la mise en œuvre de la biométrie, «les risques pour la protection des droits et libertés fondamentaux de l'individu, avant tout la question de savoir si le

but visé ne pourrait pas être atteint d'une manière moins attentatoire aux droits de la personne concernée, doivent aussi être pris en considération» lors de l'appréciation de la proportionnalité. Comme le même groupe le stipule encore «les systèmes biométriques utilisés pour le contrôle d'accès (vérification) comportent moins de dangers pour la protection des droits et libertés fondamentaux de l'individu, lorsqu'ils se basent sur des caractéristiques corporelles ne laissant pas de trace (par ex. contour de la main, mais pas empreinte digitale) ou qu'ils exploitent des caractéristiques corporelles laissant bien des traces, mais mémorisent les données biométriques sur un support qui reste en possession de la personne concernée (en d'autres termes lorsque les données ne sont pas enregistrées dans l'appareil de contrôle d'accès ou dans une base de données centralisées» [Groupe de travail «Article 29» sur la protection des données, Document de travail sur la biométrie, adopté le 1er août 2003, 12168/02/FR GT 80]).

Dans le cas présent, il s'agit d'un système de réservation pour une installation de loisirs. La biométrie est mise en œuvre pour la vérification des membres du club. On n'atteint une économicité de données qu'en collectant les données biométriques absolument nécessaires à la vérification. Les données brutes ne sont pas nécessaires pour la vérification. La comparaison avec un gabarit suffit pour vérifier si la personne est autorisée lors de la confirmation de réservation. Le fait de n'enregistrer que les gabarits biométriques, comme cela est effectué par le CT XX, est donc proportionnel du point de vue de l'économicité de données.

Les données biométriques sont liées de manière permanente aux personnes. Précisément lorsqu'ils s'agit de domaines aussi sensibles que les empreintes digitales, ces données biométriques devraient de ce fait être mémorisées dans le domaine d'influence de la personne concernée, c'est-à-dire du membre, et y rester.

De ce qui a été dit jusqu'à présent, il découle qu'il existe les trois variantes suivantes pour une réalisation du système conforme à la protection des données dans le cadre de la mise en œuvre de la biométrie pour vérifier les personnes autorisées à accéder à une installation de loisirs. Pour des caractéristiques laissant des traces (physiques ou numériques) comme les empreintes digitales ou les photographies du visage, seules les variantes a) et b) avec cartes individuelles garantissent un niveau de protection suffisant. La variante c) sans carte est par contre envisageable pour des caractéristiques biométriques ne laissant pas de trace comme le réseau veineux du doigt ou le contour de la main.

a) Décentralisation: (sur cartes)

Comme le PFPDT le stipule dans son guide concernant les systèmes de reconnaissance biométrique datant de septembre 2009, la protection de la personnalité des personnes concernées est au mieux assurée lors de la mise en œuvre de la biométrie dans le domaine privé, si

1. les données biométriques sont conservées sous forme de gabarits chiffrés sur un support sécurisé se trouvant sous contrôle individuel de la personne concernée; et
2. la personne concernée doit libérer explicitement et consciemment chaque accès aux données; et
3. la vérification de l'identité n'a lieu que sur le support sécurisé, de telle sorte que les données biométriques ne quittent à aucun moment l'environnement sécurisé du support et le contrôle de la personne concernée (comparaison biométrique sur carte, cf. guide p. 13).

b) Pseudodécentralisation: (avec cartes)

Un niveau approximativement aussi élevé quant à la protection de la personnalité peut être atteint au moyen d'une pseudodécentralisation. Cette solution a aussi été esquissée par le Tribunal administratif fédéral dans son jugement du 4 août 2009 (A-3908/2008) concernant le cas KSS. À la différence de la vraie décentralisation, les données biométriques sont certes mémorisées de manière centralisée, mais un accès logique à ces données n'est possible qu'à l'aide d'un code de correspondance mémorisé sur une carte possédée exclusivement par la personne concernée. Cela signifie en détail ce qui suit:

1. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie);
2. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec une personne identifiée ou identifiable ne puisse être établi par le maître de fichier. Des données statistiques ou accessoires peuvent leur être associées, pour autant quelles ne soient pas identifiantes;
3. le lien entre un gabarit biométrique et la personne concernée est établi uniquement avec l'autorisation expresse et libre de cette dernière lorsqu'elle fait usage de sa carte individuelle .

c) Centralisation: (sans carte)

Dans le cas où l'introduction de cartes individuelles n'est pas souhaitée dans le cadre d'une vérification biométrique des membres d'un club de loisirs, seule un système avec une centralisation des références biométriques est envisageable. Comme de tels systèmes sont théoriquement appropriés pour accomplir une identification biométrique, ils doivent respecter l'ensemble des conditions suivantes pour ne pas être jugés disproportionnés pour effectuer une pure vérification biométrique:

1. seules des caractéristiques biométriques sans trace (physique ou numérique) peuvent être exploitées;
2. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie);
3. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec d'autres données identifiantes de personnes concernées ne puisse être établi par le maître de fichier. Des données statistiques (ex: sexe) ou accessoires (ex: date d'expiration) peuvent cependant leur être associées, pour autant qu'elles ne soient pas identifiantes;
4. le lien entre un gabarit biométrique et la personne concernée est établi de manière volatile par le système de reconnaissance, uniquement pour attester de son appartenance aux membres. La suite des opérations (confirmation de réservation…) a lieu sur une base non biométrique.

En conclusion, le CT XX doit pour l'avenir choisir une des trois variantes décrites ci-dessus et la mettre en œuvre de manière appropriée, aussi pour les données déjà mémorisées de manière centralisée. La centralisation actuelle des données biométriques dans le cas présent de la réservation de courts de tennis par le CT XX est disproportionnée du point de vue du principe de l'économicité des données et du principe du traitement ménageant au mieux les données personnelles.

5.5.2.2 Publication des données de réservation sur Internet

Le système de réservation permet aux membres de procéder à la réservation des courts depuis Internet et de confirmer ensuite cette réservation sur place avec son empreinte digitale. C'est dans ce but que le système est activé sur le site du CT XX. Le PFPDT reconnaît que la réservation en ligne est d'une grande utilité pour les membres et offre par ailleurs la possibilité de rechercher et trouver des partenaires de jeu. Pour atteindre cette finalité, il paraît aussi proportionnel de mettre à disposition des membres cet accès en ligne au système de réservation.

Du point de vue du PFPDT, il n'y a par contre aucune raison d'autoriser sans restriction cet accès aux données de réservation et de permettre ainsi leur consultation par des non-membres. Cela dépasse de loin ce qui est nécessaire pour atteindre le but visé. Le PFPDT est donc d'avis que l'accès en ligne au système de réservation doit être restreint aux seuls membres du club. Une protection par mot de passe pourrait par exemple suffire. Du fait que la réservation en ligne requiert de toute façon une connexion, cette restriction ne nécessiterait qu'une modification minimale du système. On pourrait par exemple déjà exiger une connexion pour la consultation des données de réservation.

Lors de la création d'un compte d'utilisateur, le PFPDT suggère en outre qu'il soit automatiquement mentionné que le véritable nom de famille sera affiché par défaut dans le système de réservation en ligne et qu'on demande explicitement à la personne concernée s'il est d'accord avec cette pratique ou si elle préfère recourir à la possibilité de pseudonymisation du nom affiché.

En résumé, on peut constater que la publication actuelle des données de réservation sur Internet dépasse de loin ce qui est nécessaire pour atteindre le but poursuivi. Elle n'est donc pas proportionnelle par rapport au principe du traitement ménageant au mieux les données personnelles.

5.5.3 Proportionnalité temporelle – Point de départ

L'exigence de proportionnalité limite également le traitement de données sur l'échelle temporelle. Dès que les données personnelles ne sont plus utiles pour le but poursuivi, elles doivent être détruites ou anonymisées. Il faut prévoir à cet égard une destruction ou une anonymisation le plus rapidement possible.

Actuellement, des données personnelles sont enregistrées à trois endroits: sur le PC «biométrique», sur le PC du secrétariat et sur le serveur web du système de réservation. Un règlement pour la durée de conservation ou la responsabilité de destruction n'existe pour aucun de ces endroits. Jusqu'à présent, aucune destruction régulière de données n'est effectuée sur le PC «biométrique» et sur le PC du secrétariat, les données de réservation du système der réservation sont par contre détruites tous les 2-3 ans pour des raisons de place, tandis que les données de journalisation sont effacées après environ une année.

5.5.4 Jugement de la proportionnalité temporelle du point de vue du PFPDT

Le PFPDT a déjà rendu attentif lors de la visite des installations sur place au fait que la durée de conservation et la responsabilité pour la destruction des données (en particulier sensibles) plus nécessaires devaient être réglées et consignées dans un règlement, car il n'est sinon pas possible pour les personnes concernées d'estimer la durée

de conservation des données. Il existe en outre le danger effectif que la destruction des données ne soit pas suffisamment prise en considération et que celles-ci soient éternellement conservées.

Les gabarits sur le PC «biométrique» et les données des membres sur le PC du secrétariat doivent être détruites dès qu'elles ne sont plus nécessaires. Cela est au plus tard le cas lorsqu'un membre donne sa démission. La destruction des données lors d'une démission doit par conséquent d'une part être arrêtée dans le règlement et d'autre part être enregistrée dans les processus standard pour de tels cas. Pour le PFPDT, il n'y a en apparence aucune raison qui justifierait une durée de conservation de 2-3 ans pour les données de réservation et d'un an pour les données de journalisation du système de réservation.

Le PFPDT estime donc que les durées de conservation sont disproportionnellement longues et doivent être réduites à une mesure appropriée. Le CT XX doit ainsi faire une proposition au PFPDT pour déterminer comment les délais de destruction doivent être fixés et comment ces délais sont ensuite (techniquement) mis en œuvre. À part la destruction des données mentionnées ci-dessus, il faut aussi régler celle des sauvegardes existantes de ces données.

5.6 Finalité du traitement

5.6.1 Point de départ

Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par la loi ou qui ressort des circonstances (art. 4 al. 3 LPD). Comme une modification du but du traitement n'est pas contrôlable par les personnes concernées à cause de la centralisation des données biométriques, il faut privilégier des solutions techniques qui garantissent suffisamment le respect de la finalité.

5.6.2 Jugement du point de vue du PFPDT

De par la centralisation actuelle des gabarits biométriques, on ne peut pas totalement exclure un détournement de finalité lors du traitement de ces données. Cela est entre autre possible, car les données ne se trouvent pas dans la sphère d'utilisation des personnes concernées. Un détournement de finalité par liaison avec d'autres fichiers ou par communication à un tiers externe serait possible. Même si on tient compte du fait qu'aucunes données brutes mais uniquement des gabarits biométriques sont stockés dans la base de données, on doit également renoncer à la mémorisation actuelle centralisée des données biométriques à cause du principe de finalité et choisir une des variantes mentionnées au chiffre 5.5.2.1.

5.7 Exactitude des données (fiabilité, applicabilité)

5.7.1 Point de départ

Le processus de comparaison entre données de référence et données présentées (ici des gabarits d'empreintes digitales) se base sur un calcul de probabilités et fournit une valeur de concordance, qui doit être supérieure à un seuil prédéfini, pour que la personne soit reconnue. De cette seule valeur de seuil dépendent les deux taux «False Rejection Rate (FFR)» et «False Acceptance Rate (FAR)» de manière inversement proportionnelle. Pour des motifs de protection de la personnalité, on devrait minimiser avant tout le FAR, sans cependant trop fortement péjorer le FRR. Le choix d'une valeur optimale du seuil d'acceptation pour atteindre une fiabilité suffisante du système biométrique global n'est donc pas facile à effectuer.

Il ne faut également pas négliger le fait que certains utilisateurs (à cause de membres manquants, blessures, cicatrices ou à cause de leur jeunesse/vieillesse) ne présentent pas de caractéristiques biométriques (ou alors de qualité insuffisante) pour accomplir une telle vérification. Pour ces personnes, un scénario alternatif doit être prévu, sans que cela puisse conduire à une discrimination des personnes concernées.

5.7.2 Jugement du point de vue du PFPDT

Pour des raisons de protection des données, le taux FAR devrait être minimisé, sans pour autant trop péjorer le taux FRR. Un seuil d'acceptation optimal doit en outre être choisi. Chaque système biométrique présente un certain taux (non nul) de FAR. La vérification ne peut de ce fait avoir lieu de manière entièrement fiable. Le système du CT XX extrait 12 minuties par gabarit biométrique, ce qui est à nos yeux tout juste suffisant. Des tests sur place ont néanmoins démontré que le système fonctionne pour l'instant à satisfaction.

Des problèmes apparaissent parfois aussi auprès de personnes dont certaines caractéristiques biométriques manquent ou ne sont que difficilement lisibles (enrôlement). Pour de telles exceptions, il faut planifier et mettre en œuvre une applicabilité équivalente du système de reconnaissance. Une telle alternative existe dans le cas présent. Au lieu d'une vérification au moyen d'empreintes digitales, un NPI est utilisé. Cette alternative est pour les personnes concernées équivalentes aussi bien du point de vue du coût que de celui de la manipulation. Il y a manifestement déjà des membres qui ne veulent ou ne peuvent pas utiliser le système biométrique et confirment par conséquent leurs réservations à l'aide d'un NPI. Cela fonctionne sans problème.

L'exactitude des données est ainsi assurée par le système de réservation. Le PFPDT n'a ici pas d'autres remarques.

5.8 Sécurité des données

5.8.1 Point de départ

Selon l'art. 7 LPD, les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées. Il faut en particulier garantir la confidentialité, la disponibilité et l'intégrité des données personnelles. Ces exigences ne sont plus satisfaites, si des personnes non autorisées peuvent aisément accéder aux données ou si un appareil étranger peut capturer ou manipuler ces données. La sécurité des données est sous la responsabilité de l'organisme qui possède la maîtrise sur les données personnelles (art. 8 al. 1 de l'ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993 (OLPD; RS 235.11).

Comme déjà mentionné, le PC «biométrique» et le PC du secrétariat se trouvent chacun dans un local du clubhouse accessible depuis l'extérieur et protégé seulement par un simple cadenas. 5-6 personnes ont un accès physique au PC «biométrique», toutefois 2-3 d'entre elles n'ont pas pu être nommées précisément. 11 personnes ont un accès physique au PC du secrétariat en dehors des heures d'ouverture, tandis que quiconque peut pénétrer dans le bureau pendant les heures d'ouverture, le PC n'étant en principe pas laissé sans surveillance et l'accès logique aux données qu'il contient étant protégé par mot de passe.

Le PC «biométrique» et le PC du secrétariat, au bénéfice d'un accès Internet (ADSL), sont reliés entre eux par un réseau sans fil (WiFi). Le réseau WiFi est sécurisé par le protocole WPA (WPA2 depuis mars 2010). Le mot de passe WiFi est communiqué aux membres qui le demandent, afin que ceux-ci puissent accéder à Internet depuis leur téléphone ou ordinateur pendant leur séjour sur le terrain du club.

À partir du PC du secrétariat, il est possible d'accéder aux gabarits biométriques par le biais d'une partition partagée cachée sur le PC «biométrique».

5.8.2 Jugement du point de vue du PFPDT

Le PFPDT juge insuffisante la protection physique du PC «biométrique» et du PC du secrétariat. Les portes y compris les cadenas peuvent être forcés sans grand effort. Les deux PC ne sont ainsi pas physiquement sécurisés comme ils devraient l'être, et un vol de données ou même d'un boîtier PC complet serait facilement envisageable. Cela doit être pour le PFPDT urgemment amélioré, particulièrement eu égard à la sensibilité des données stockées sur ces PC.

L'accès physique aux PC «biométrique» et du secrétariat n'est pas réglé de manière assez claire. Pour les deux postes, il faut par conséquent établir une liste définissant clairement les ayants droit, le nombre de ces derniers devant par ailleurs être réduit à un

minimum. La même remarque est valable pour les droits d'accès logique aux données de ces ordinateurs (comptes d'utilisateur), ainsi que pour l'accès physique et logique aux sauvegardes des données.

Le PFPDT considère en outre problématique le fait que la transmission de données personnelles biométriques a lieu par WiFi, protocole qui n'offre pas les mêmes standards de sécurité qu'une transmission par câble, surtout que ce réseau WiFi peut également être utilisé par les membres pour un accès privé à Internet. Il propose par conséquent que la liaison entre le PC «biométrique» et le PC du secrétariat, de même que la liaison entre ce dernier et le modem/routeur ADSL, soient établies par câble et que le réseau WiFi ne soit à l'avenir plus qu'utilisé pour permettre aux membres d'accéder à Internet. La transmission des données personnelles (biométriques) aura ainsi lieu de manière plus sûre et séparée du trafic Internet occasionné par les membres.

5.9 Droit d'accès

5.9.1 Point de départ

Selon l'art. 8 LPD, toute personne peut demander au maître du fichier si des données la concernant sont traitées.

Chez le CT XX, les membres peuvent s'adresser à tout moment au président, pour obtenir un droit de regard sur leur gabarit biométrique. Le président s'est engagé à étendre ce droit d'accès à l'ensemble des données traitées sur les membres.

5.9.2 Jugement du point de vue du PFPDT

Avec l'extension du droit d'accès à toutes les données sur les membres, les droits correspondants des membres seront garantis. Le PFPDT n'a pas d'autres remarques à ce sujet.

6. Résultats

Sur la base de l'analyse des documents qui nous ont été remis et du contrôle effectué le 11.02.2010 selon l'art. 29 LPD, le PFPDT parvient à un jugement global critique du système biométrique de réservation. Le contrôle de protection des données a révélé que le traitement de données personnelles effectué par le CT XX depuis l'introduction du système biométrique de réservation n'a pas lieu de manière entièrement conforme aux exigences de protection des données. Lors de son contrôle, le PFPDT est tombé sur des états de fait qui nécessitent une amélioration ou une modification du point de vue de la protection des données.

Partant de ce constat global, le PFPDT arrête son jugement global à l'attention du CT XX sous la forme de:

- Constatations et/ou
- Recommandations au sens de l'art. 29 al. 3 LPD.

6.1 Données biométriques en tant que données personnelles

Avec des données biométriques d'empreintes digitales, il s'agit de données personnelles selon l'art. 3 lit. a LPD. Des données biométriques sous forme brute ou dérivée (gabarit) rendent une personne identifiable. Leur collecte laisse en général – en particulier celle d'empreintes digitales – des traces. La collecte de données biométriques brutes (ou dérivées) est ainsi susceptible de produire un profil de mouvements de la personne concernée. De ce fait, il existe lors de la collecte de données biométriques pour la personne concernée un grand potentiel d'atteintes à la personnalité.

6.2 But du traitement de données

Chaque traitement de données personnelles peut entraîner une atteinte au droit à la protection de la sphère privée selon l'art. 13 al. 2 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.; RS 101). Un tel traitement nécessite par conséquent un motif justificatif particulier. Des considérations pratiques ou une simple convivialité pour les clients ne représentent pas un motif justificatif suffisant pour le traitement de données biométriques.

Selon les indications du CT XX, la saisie des données biométriques vise exclusivement la lutte automatique contre les abus de réservation et d'utilisation des courts de tennis. L'avantage pour le CT XX résiderait dans le fait qu'aucune vérification personnelle de l'identité des joueurs ne doit être effectuée (par exemple par l'exploitation d'une réception) lors de la réservation et l'utilisation des courts. Le nouveau système biométrique de réservation remplace l'ancien système basé sur un NPI, avec lequel de nombreux cas d'abus auraient été constatés. Selon les indication du CT XX, le nombre de membres a fortement augmenté depuis l'introduction du nouveau système, tandis que les courts ont été moins utilisés durant la même période, ce qui serait en rapport avec l'absence de possibilités d'abus. L'avantage pour les membres réside dans le fait qu'ils ne doivent pas être porteurs d'une carte de membre. Les réservations depuis Internet restent en outre possibles, comme avec le système précédent.

Le nouveau système biométrique de réservation du CT XX poursuit des buts plausibles. Le PFPDT aimerait cependant exprimer ses sérieuses préoccupations quant à la question de savoir s'il n'existe pas d'autres alternatives pour éviter les mêmes abus, mais qui seraient moins attentatoires aux droits de la personnalité des personnes

concernées (cf. à cet égard aussi le résultat de la vérification de proportionnalité au chiffre 6.5.1.1, Recommandation 2).

6.3 Licéité du traitement de données / Consentement des personnes concernées

Le traitement de données biométriques requiert un motif justificatif (art. 12 et 13 LPD). Dans le cas présent, le consentement de la personne concernée entre en ligne de compte. Le système biométrique de réservation a été introduit suite à une décision correspondante d'une AG. Une alternative valable a été offerte aux membres qui n'étaient pas d'accord avec le système, de sorte que qu'on peut partir de l'idée que les membres qui utilisent le système biométrique ont donné leur consentement.

Du point de vue du PFPDT, il manque cependant d'importantes informations, comme en particulier les modalités de traitement, l'indication explicite de l'existence d'une alternative sans exploitation de données biométriques et le fait que le nom de famille des membres du club peut être publié dans le système de réservation (voir plus loin 6.5.1.2).

Recommandation 1:

a) Le CT XX doit établir d'ici au 31.12.2010 une feuille d'information expliquant les modalités de traitement des données biométriques, la possibilité d'une alternative sans exploitation de données biométriques, ainsi que le fait que le nom de famille des membres est publié dans le système de réservation, à moins que l'option de pseudonymisation n'ait été choisie. Les points principaux du traitement de données doivent être décrits, par exemple le détail de l'utilisation des gabarits biométriques, le lieu de stockage des données, le moment de leur destruction, la journalisation des transactions, les différentes personnes ayant accès aux données et les éventuels destinataires de données.

b) Cette feuille d'information doit en outre être signée par la direction du CT XX et dotée d'un contrôle de versions.

c) Cette feuille d'information doit enfin être remise immédiatement à tous les membres existants et automatiquement à tous les nouveaux arrivants avant leur enrôlement. Le CT XX doit bien entendu veiller à ce que chaque nouveau membre dispose d'un temps suffisant pour prendre connaissance de ce document avant son inscription.

6.4 Traitement selon la bonne foi / Transparence

L'enrôlement n'est possible qu'avec le concours du membre. Sans sa participation, aucune donnée biométrique ne peut être collectée par le CT XX. Le traitement de données a lieu pour ce point de manière transparente et est reconnaissable par la personne concernée.

On doit néanmoins regretter que l'information des membres quant aux modalités de traitement des données soit insuffisante. Les membres ont certes été informés à l'occasion de l'AG oralement par le président du club, puis au moyen de la notice d'utilisation du système. Pour un traitement de données aussi transparent que possible, il faudrait remettre une feuille d'information, en plus des explications orales du président du club et de la notice d'utilisation informant purement sur la manipulation correcte du système. Cette feuille d'information doit décrire au minimum ce qui passe avec les données personnelles et qu'une alternative sans collecte de données biométriques existe (cf. Recommandation 1).

6.5 Proportionnalité du traitement de données

6.5.1 Proportionnalité matérielle

6.5.1.1 Centralisation des données biométriques

La mise en œuvre de processus biométriques dans le domaine privé représente en fonction de leur conception dans le cas concret d'espèce une atteinte plus ou moins intensive aux droits de la personnalité des personnes concernées. Avant la mise en œuvre de tels processus biométriques, il faut donc en principe toujours vérifier si d'autres mesures appropriées, mais moins attentatoires aux droits fondamentaux des personnes concernées, ne permettraient pas également d'atteindre le but visé. Par ailleurs, il faut déjà lors du choix et de la conception du processus biométrique veiller à choisir un système qui soit le plus économique possible en données et qui reste dans un rapport raisonnable avec le but visé.

Dans le cas présent, il s'agit d'un système de réservation pour des courts de tennis. La biométrie est mise en œuvre pour la vérification des membres du club. On n'atteint une économicité de données qu'en collectant les données biométriques absolument nécessaires à la vérification.

Pour la mise en œuvre du nouveau système de réservation, des gabarits sont générés à partir des empreintes digitales des membres, puis stockés dans une base de données centrale. Les données brutes, c'est-à-dire les images originales des empreintes

digitales, ne sont pas conservées. La limitation de n'enregistrer que les gabarits biométriques, comme cela est effectué par le CT XX, est donc proportionnelle du point de vue de l'économicité de données.

Les données biométriques sont liées de manière permanente aux personnes et susceptibles de produire un profil de mouvements de la personne concernée. Précisément lorsqu'il s'agit de domaines aussi sensibles que les empreintes digitales, ces données biométriques devraient de ce fait être mémorisées dans le domaine d'influence de la personne concernée respectivement de l'utilisateur. Le principe de la proportionnalité matérielle exige que pour les systèmes biométriques capables de fonctionner également sans centralisation des données, les caractéristiques biométriques ne soient dans la mesure du possible pas sauvegardées dans une base de données centrale, mais bien plutôt sur un support exclusivement accessible au seul utilisateur.

De ce qui a été dit jusqu'à présent, il découle qu'il existe les trois variantes suivantes pour une réalisation du système conforme à la protection des données dans le cadre de la mise en œuvre de la biométrie pour vérifier les personnes autorisées à accéder à une installation de loisirs. Pour des caractéristiques laissant des traces (physiques ou numériques) comme les empreintes digitales ou les photographies du visage, seules les variantes a) et b) avec cartes individuelles garantissent un niveau de protection suffisant. La variante c) sans carte est par contre envisageable pour des caractéristiques biométriques ne laissant pas de trace comme le réseau veineux du doigt ou le contour de la main.

a) Décentralisation: (sur cartes)

Comme le PFPDT le stipule dans son guide concernant les systèmes de reconnaissance biométrique datant de septembre 2009, la protection de la personnalité des personnes concernées est au mieux assurée lors de la mise en œuvre de la biométrie dans le domaine privé, si

1. les données biométriques sont conservées sous forme de gabarits chiffrés sur un support sécurisé se trouvant sous contrôle individuel de la personne concernée; et
2. la personne concernée doit libérer explicitement et consciemment chaque accès aux données; et
3. la vérification de l'identité n'a lieu que sur le support sécurisé, de telle sorte que les données biométriques ne quittent à aucun moment l'environnement sécurisé du support et le contrôle de la personne concernée (comparaison biométrique sur carte, cf. guide p. 13).

b) Pseudodécentralisation: (avec cartes)

Un niveau approximativement aussi élevé quant à la protection de la personnalité peut être atteint au moyen d'une pseudodécentralisation. Cette solution a aussi été esquissée par le Tribunal administratif fédéral dans son jugement du 4 août 2009 (A-3908/2008) concernant le cas KSS. À la différence de la vraie décentralisation, les données biométriques sont certes mémorisées de manière centralisée, mais un accès logique à ces données n'est possible qu'à l'aide d'un code de correspondance mémorisé sur une carte possédée exclusivement par la personne concernée. Cela signifie en détail ce qui suit:

1. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie);
2. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec une personne identifiée ou identifiable ne puisse être établi par le maître de fichier. Des données statistiques ou accessoires peuvent leur être associées, pour autant quelles ne soient pas identifiantes;
3. le lien entre un gabarit biométrique et la personne concernée est établi uniquement avec l'autorisation expresse et libre de cette dernière lorsqu'elle fait usage de sa carte individuelle .

c) Centralisation: (sans carte)

Dans le cas où l'introduction de cartes individuelles n'est pas souhaitée dans le cadre d'une vérification biométrique des membres d'un club de loisirs, seule un système avec une centralisation des références biométriques est envisageable. Comme de tels systèmes sont théoriquement appropriés pour accomplir une identification biométrique, ils doivent respecter l'ensemble des conditions suivantes pour ne pas être jugés disproportionnés pour effectuer une pure vérification biométrique:

1. seules des caractéristiques biométriques sans trace (physique ou numérique) peuvent être exploitées;
2. les données biométriques sont conservées de manière centralisée sous forme de gabarits chiffrés (et non de données brutes comme une image ou une photographie);

3. les gabarits biométriques sont conservés de telle sorte qu'aucun lien avec d'autres données identifiantes de personnes concernées ne puisse être établi par le maître de fichier. Des données statistiques (ex: sexe) ou accessoires (ex: date d'expiration) peuvent cependant leur être associées, pour autant qu'elles ne soient pas identifiantes;

4. le lien entre un gabarit biométrique et la personne concernée est établi de manière volatile par le système de reconnaissance, uniquement pour attester de son appartenance aux membres. La suite des opérations (confirmation de réservation…) a lieu sur une base non biométrique.

Recommandation 2:

a) À l'avenir, mais au plus tard le 30.06.2011, le CT XX renonce à l'actuelle mémorisation centralisée de gabarits biométriques d'empreintes digitales.

b) Si le CT XX souhaite maintenir l'utilisation de données biométriques pour la vérification des membres dans le système de réservation, alors il faut que:

- les données biométriques, y compris celles qui ont déjà été enregistrées centralement, soient mémorisées sur un support restant dans la sphère d'utilisation et sous contrôle de la personne concernée (solution minimale de «comparaison biométrique sur carte», cf. p. 13 du guide); ou

- les données biométriques soient centralisées sous forme de gabarits chiffrés, toutefois sans aucun lien avec d'autres données personnelles, de telle sorte qu'une correspondance avec une personne identifiée ou identifiable ne soit possible qu'avec l'autorisation explicite et consciente de la personne concernée par l'usage de sa carte individuelle; ou

- seules des caractéristiques biométriques ne laissant aucune trace (physique ou numérique) soient exploitées, pour autant que les données soient mémorisées sous forme de gabarits biométriques chiffrés, sans aucune correspondance permanente avec d'autres données identifiantes de personnes concernées.

6.5.1.2 Publication des données de réservation sur Internet

Une publication de données personnelles sur Internet est toujours liée à des risques particuliers. De ce fait, le but de la publication doit être au préalable soigneusement examiné et la publication doit être limitée aux seules données absolument nécessaires pour atteindre ce but. À chaque fois que possible, l'accès doit par exemple être restreint par mot de passe aux seules personnes qui en ont vraiment besoin pour atteindre le but visé.

Dans le cas présent, la publication sur Internet sert à permettre aux membres du club d'effectuer une réservation en ligne. Cette finalité peut être atteinte sans restrictions, si l'accès est limité aux seuls membres du club. La réalisation technique de cette limitation d'accès ne devrait poser que peu de problèmes, car l'activation d'une réservation requiert maintenant déjà une connexion. La limitation peut certainement être atteinte au moyen d'une identification d'utilisateur avec authentification par mot de passe. Un protocole chiffré et éprouvé comme SSL (Secure Socket Layer) permet aujourd'hui d'assurer la confidentialité des transmissions de données. La longueur des clés doit alors s'élever au moins à 128 bit.

Recommandation 3:

L'accès au système de réservation en ligne doit être protégé par mot de passe et par transmission chiffrée (état actuel de la technique) aux seuls membres du club d'ici au 31.12.2010.

Pour la réservation en ligne, la nomination des personnes n'est en outre pas indispensable. Il suffit de pouvoir reconnaître si un court est libre ou occupé. La plus-value de pouvoir trouver un partenaire de jeu par son vrai nom doit avoir lieu sur une base volontaire. Si le véritable nom est cependant celui qui est affiché par défaut, il y a le risque que beaucoup de membres laissent apparaître ce nom par méconnaissance ou confort, sans qu'ils soient véritablement d'accord avec la publication de leur nom dans le système de réservation. C'est la raison pour laquelle les membres doivent être rendus attentifs à ce fait et surtout à la possibilité de pseudonymisation (cf. à cet égard la recommandation 1a).

6.5.2 Proportionnalité temporelle

À l'heure actuelle, le CT XX n'effectue aucune destruction régulière de données. Les données du système de réservation sont effacées tous les 2-3 ans pour des raisons de place, les autres données ne sont jusqu'à présent jamais effacées. Aucun délai de destruction n'est prescrit nulle part. La proportionnalité temporelle n'est donc pas satisfaite.

Recommandation 4:

Le CT XX doit introduire des délais de destruction pour toutes les données sur les membres, y compris celle enregistrées sur des supports de sauvegarde (backup). À cet effet, il soumet au PFPDT une proposition de règlement des délais de destruction des données et entreprend les adaptations techniques nécessaires pour mettre en œuvre ce règlement avant le 31.12.2010.

6.6 Finalité du traitement

De par la centralisation actuellement pratiquée des gabarits biométriques, on ne peut pas totalement exclure un détournement de la finalité (i.e. un traitement dépassant l'empêchement des abus) de ces données délicates. Un détournement de finalité par liaison avec d'autres fichiers ou par communication à un tiers externe serait possible. Comme une modification du but du traitement des données biométriques centralisées n'est pas contrôlable par les personnes concernées, il faut privilégier des solutions techniques permettant de garantir au mieux le respect de la finalité. Du point de vue du respect de la finalité, il faut prévoir la mémorisation décentralisée des données biométriques sur un support se trouvant dans la sphère d'utilisation de la personne concernée. On peut ici se référer à la recommandation 2.

6.7 Exactitude des données (fiabilité, applicabilité)

Pour des raisons de protection des données, le taux FAR devrait être minimisé, sans pour autant trop péjorer le taux FRR. Un seuil d'acceptation optimal doit en outre être choisi. Chaque système biométrique présente un certain taux (non nul) de FAR. La vérification ne peut de ce fait avoir lieu de manière entièrement fiable.

Pour les personnes dont certaines caractéristiques biométriques manquent ou ne sont que difficilement lisibles (jeunesse/vieillesse, cicatrices, etc.), il faut planifier et mettre en œuvre une applicabilité équivalente du système de reconnaissance.

Le nombre des minuties par gabarit utilisées par le CT XX se trouve dans la fourchette de tolérance. Les personnes qui ne peuvent pas utiliser pour cause de caractéristiques manquantes ou de qualité insuffisante pour le système ont la possibilité d'effectuer leur réservation au moyen d'un NPI et jouissent ainsi d'une alternative équivalente. Le PFPDT n'a pas de remarques au sujet de l'exactitude des données, à part le fait qu'il est d'avis que la centralisation des données n'est pas proportionnelle et par conséquent qu'une décentralisation des données sur un support restant dans la sphère d'utilisation de la personne concernée s'impose (cf. recommandation 2).

6.8 Sécurité des données

La sécurité des données chez le CT XX n'est pas suffisamment garantie, précisément eu égard à la sensibilité des données personnelles utilisées. Les ordinateurs doivent être mieux sécurisés physiquement, afin de minimiser la probabilité d'un vol. Les droits d'accès physique et logique doivent en outre être mieux réglés et également réduits en nombre, toujours afin de limiter les risques. Une transformation du réseau devrait enfin améliorer la sécurité des transmissions de données.

Recommandation 5:

Afin d'améliorer la sécurité actuellement insuffisante des données, en particulier eu égard à leur sensibilité, le CT XX a jusqu'au 31.12.2010 pour:

a. améliorer la sécurité physique du PC «biométrique» et du PC du secrétariat par des mesures appropriées.

b. réglemente les droits d'accès physique au PC «biométrique» et au PC du secrétariat, en réduisant le nombre d'ayants droit à un strict minimum.

6.9 Droit d'accès

Les membres ont en tout temps la possibilité de consulter leurs données personnelles et de les faire actualiser si nécessaire. Le droit d'accès des membres étant garanti, le PFPDT n'a pas de remarques à ce sujet.

7. Conclusions

7.1 Concernant le contrôle de la collecte de données biométriques

Dans le but d'endiguer les abus de réservation et d'utilisation des courts de tennis, le CT XX a introduit durant l'été 2009 un nouveau système de réservation, collectant et mémorisant des gabarits biométriques d'empreintes digitales, en plus des renseignements usuels sur les membres.

Le contrôle de protection des données effectué a fourni au PFPDT un aperçu détaillé du nouveau système biométrique de réservation. La documentation mise à disposition par le CT XX a permis au PFPDT d'examiner les traitements de données correspondants quant au respect des dispositions de protection des données.

Le PFPDT arrive à un jugement global critique de ce système biométrique de réservation. Le contrôle de protection des données a montré que le traitement de données personnelles effectué par le CT XX depuis l'introduction du nouveau système biométrique de réservation n'est pas en tout point conforme aux exigences de protection des données. Le PFPDT a expliqué avec justification, tout ce qui devait être modifié ou amélioré.

7.2 Procédure et prochaines étapes

Le présent rapport de contrôle comprend une série de constatations et de recommandations formulées par le PFPDT sur la base des conclusions de l'audit effectué. Le rapport complet de contrôle sera remis au CT XX pour prise de connaissance. Dans un délai de 30 jours après réception, le CT XX devra communiquer au PFPDT s'il a des

remarques à formuler et, s'il accepte les recommandations, la proposition de règlement de délais de destruction (cf. recommandation 4). Au cas où le CT XX refuserait ou ne suivrait pas les recommandations, le PFPDT peut porter l'affaire devant le Tribunal administratif fédéral pour décision (art. 29 al. 4 LPD).

En considération de la sensibilité des données personnelles traitées et des réactions de certains membres du club, le contrôle du nouveau système du CT XX quant au respect des exigences de protection des données s'est avéré très utile. Les constatations et recommandations faites par le PFPDT montrent la direction à suivre par d'autres exploitants privés de systèmes biométriques dans le domaine des clubs de loisirs.

Pour les raisons susmentionnées, il existe un intérêt fondamental à sensibiliser le public à ce genre de collecte de données et à l'informer en particulier sur le contrôle de protection des données effectué chez le CT XX et sur les résultats obtenus. Se basant sur l'art. 30 al.2 LPD, le PFPDT va donc rendre public sur son site (www.edoeb.admin.ch) et sous une forme adaptée et anonymisée le présent rapport de contrôle concernant la collecte de données biométriques dans le cadre de la réservation de courts du club de tennis du CT XX. Il va de soi que cette publication n'aura lieu que sous réserve que du point de vue du CT XX (avec l'accord du fournisseur du système), aucune donnée confidentielle qui pourrait révéler des secrets d'affaire ou influencer la capacité concurrentielle ne sera communiquée. Le CT XX est prié de vérifier que le rapport de contrôle ne contient pas de tels contenus confidentiels et de confirmer cet état de fait par écrit au PFPDT dans un délai de 30 jours.

Nous vous prions de prendre bonne note de ce qui précède et vous remercions encore de votre bonne collaboration durant l'établissement des faits.

4.2 Principe de la transparence

4.2.1 Recommandation adressée à l'Office fédéral de la santé: «Déclarations d'intérêts des membres de la commission»

Voir chiffre 4.2.1 de la partie en langue allemande

4.2.2 Recommandation adressée à l'Office fédéral des assurances sociales: «Liste de contrôle AI» (I)

Voir chiffre 4.2.2 de la partie en langue allemande

4.2.3 Recommandation adressée à Swissmedic: «Dossiers d'autorisations»

Berne, le 30 mars 2010

Recommandation[1]

émise au titre

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

concernant les demandes en médiation introduites

Requérante A
Requérante B
Requérante C
Requérante D
Requérante E

contre

Swissmedic
Institut suisse des produits thérapeutiques

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

1. Par courrier du 7 décembre 2007, se fondant sur la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans; RS 152.3), les requérantes A et B (il s'agissait de scientifiques) ont requis de l'Institut suisse des

[1] Traduction du texte original allemand

produits thérapeutiques (ci-après: Institut Swissmedic) l'accès à certains documents traitant de la mise sur le marché de médicaments (ci-après: dossiers d'autorisation). La demande était accompagnée d'une liste des documents souhaités.

2. Par courrier du 21 décembre 2007, l'Institut Swissmedic a informé les requérantes A et B que, eu égard au nombre des documents concernés, il lui faudrait plusieurs jours de travail pour les réunir et qu'il ne serait donc pas en mesure de tenir le délai légal de 20 jours. Il leur a également indiqué qu'il était fort probable que la facture dépasserait nettement 2000 francs.

3. Par courrier du 4 mars 2008, l'Institut Swissmedic a adressé aux requérantes A et B une «prise de position provisoire», par laquelle il leur faisait part de ses estimations quant à leurs chances de se voir accorder ou non l'accès aux différents documents concernés. Il leur indiquait par ailleurs que les émoluments s'élèveraient à 10'000 francs au moins, et les priait de lui confirmer leur demande de consultation, conformément à l'art. 16, al. 2 de l'ordonnance sur le principe de la transparence dans l'administration (ordonnance sur la transparence, OTrans; RS 153.31).

4. Le 10 juin 2008, les requérantes A et B ont formé une nouvelle demande auprès de l'Institut Swissmedic, qui ne portait plus que sur certains des documents dont elles avaient précédemment requis la consultation.

5. Par courrier du 26 juin 2008, l'Institut Swissmedic a fait savoir aux requérantes A et B que, ayant soumis leur demande à un examen minutieux, il avait constaté qu'elle demanderait un travail et donc un temps considérables, de sorte que les documents ne pourraient être réunis avant la mi-septembre. Il les a également avisées qu'il leur en coûterait 10'000 francs au moins d'émoluments. Le 3 juillet 2008, donc dans le délai prescrit, les requérantes A et B ont répondu à l'Institut Swissmedic qu'elles maintenaient néanmoins leur demande. Le même jour, elles ont saisi le Préposé fédéral à la protection des données et à la transparence (ci-après: Préposé) d'une requête en médiation portant sur le montant des émoluments que l'Institut Swissmedic entendait mettre à leur charge.

6. Par courrier du 12 septembre 2008, l'Institut Swissmedic a indiqué aux requérantes A et B que leur demande avait manifestement pour objet, non pas d'obtenir des informations sur tel ou tel médicament, mais à savoir comment il appliquait la loi sur la transparence. L'Institut Swissmedic a ajouté à cet égard qu'«au vu du volume énorme, des multiples thématiques concernées […], des questions délicates qui se posent à cet égard et occasionnent une charge de travail immense pour Swissmedic, ainsi que du fait que les requérantes ne s'intéressent pas aux informations en tant que telles mais souhaitent faire le point sur des pratiques qui ne sont pas encore bien établies, nous considérons que la demande en question constitue un abus de droit.»

Conclusion: «Swissmedic considère votre demande d'accès à des documents officiels […] comme constituant un abus de droit, raison pour laquelle l'institut ne traitera pas cette dernière sur le fond.»

Par courrier du 3 octobre 2008, les requérantes A et B ont saisi le Préposé d'une seconde requête en médiation.

7. Par mémoire du 5 janvier 2009, les requérantes A et B ont déposé auprès du Tribunal administratif fédéral (ci-après: TAF) un recours pour retard injustifié contre le fait que le Préposé n'avait rendu aucune recommandation. Dans son arrêt du 16 avril 2009 (A-75/2009), le TAF a reconnu qu'il y avait effectivement retard injustifié, et il a invité le Préposé à procéder à la médiation et à établir sa recommandation sur les demandes en médiation dans un délai de trente jours.

8. Dans le cadre de deux audiences de médiation organisées par le Préposé, les requérantes A et B ont conclu avec l'Institut Swissmedic un accord sur le nombre des documents à consulter, sur un accès échelonné dans le temps et sur les émoluments à acquitter. Il était notamment prévu que l'Institut Swissmedic, dans une première étape et «sous réserve des dispositions de la LTrans», autorise avant la fin novembre 2009 l'accès aux dossiers d'autorisation de deux médicaments. La médiation ayant abouti, le Préposé n'était plus tenu d'établir de recommandation.

9. Dans le cadre de l'application de cet accord, l'Institut Swissmedic, conformément à l'obligation prévue à l'art. 11 LTrans, a entendu les entreprises pharmaceutiques concernées (requérantes C, D[2] et E), et il leur a soumis les documents concernés en les assortissant de propositions de passages à caviarder. Dans la réponse qu'elles ont adressée à l'Institut Swissmedic, les requérantes C, D et E se sont opposées à la demande d'accès, en faisant valoir les arguments suivants:

   - les requérantes C et D (défendues par le même avocat) ont soutenu que les pièces constitutives de leurs dossiers d'autorisation contenaient des secrets au sens de l'art. 7, al. 1, let. g LTrans et que non seulement leur publication «porterait atteinte à leur sphère privée», mais qu'elle entraînerait un risque d'usage abusif des données concernées, notamment pour ce qui est des documents internes à Swissmedic, des entreprises concurrentes pouvant notamment exploiter les observations qu'ils contenaient et se faire une idée des intentions commerciales de C et D. Elles ont par ailleurs fait valoir que les dossiers d'autorisation étaient protégés par l'art. 39, al. 3 de l'accord sur les ADPIC[3] et l'art. 12 LPTH[4]. C et D ont demandé, à titre principal, que la demande d'accès soit reje-

[2] La requérante D était partie à la médiation au titre de tiers concerné parce qu'elle a repris de C l'un des médicaments visés par la demande des requérantes A et B.
[3] Accord sur les ADPIC (accord du 15 avril 1994 instituant l'Organisation mondiale du commerce, RS 0.632.20)
[4] Loi fédérale du 15 décembre 2000 sur les médicaments et les dispositifs médicaux (loi sur les produits thérapeutiques, LPTh, RS 812.21)

tée sans réserve, et à titre subsidiaire, qu'il lui soit donné suite en partie, avec caviardage de passages supplémentaires.

- La requérante E a déclaré d'emblée qu'elle ne pouvait répondre favorablement à la demande de consultation. Elle a ensuite invoqué un secret des affaires couvrant la totalité des informations et documents qui participent à la procédure d'autorisation de son médicament, en ajoutant que la publication de dossiers d'autorisation fournirait de manière injustifiée aux entreprises concurrentes des informations susceptibles notamment de leur procurer un avantage indu, à quoi l'art. 39, al. 3 de l'accord sur les ADPIC permet de s'opposer.

10. Sur la base des prises de positions qui lui avaient été adressées, l'Institut Swissmedic a caviardé des passages supplémentaires dans certaines pièces constitutives des dossiers d'autorisation, avant d'informer les requérantes C, D et E qu'il maintenait son intention de donner partiellement accès aux dossiers et d'attirer leur attention sur la possibilité que leur offrait l'art. 13, al. 1, let. c LTrans de déposer une demande en médiation. C, D et E ont alors déposé une telle demande en médiation auprès du Préposé.

11. L'Institut Swissmedic a simultanément informé les requérantes A et B du refus des entreprises pharmaceutiques concernées de donner accès à leurs documents. Se fondant également sur l'art. 13, al. 1, let. c LTrans, les requérantes A et B ont alors déposé elles aussi une demande en médiation auprès du Préposé.

12. À la demande du Préposé, l'Institut Swissmedic lui a transmis ses prises de position pour les différentes demandes de médiation, assortis d'une liste détaillée des documents concernés où il indiquait quels passages il se proposait de caviarder et pourquoi. L'Institut Swissmedic a également admis que la LTrans était a priori applicable aux dossiers d'autorisation, non sans préciser toutefois que la question de savoir s'il fallait ou non laisser consulter des documents relevant de procédures d'autorisation était pour lui délicate à trancher, car il n'était pas en mesure d'apprécier si, lorsqu'elles invoquaient le secret, les entreprises concernées étaient effectivement fondées à le faire, et quels poids il fallait accorder aux intérêts ainsi mis en avant. Ces difficultés étaient notamment dues au fait que l'intérêt au maintien du secret ne pouvait s'apprécier à la lumière du seul document ou information faisant l'objet de la décision, et qu'il fallait le replacer dans le contexte d'un ensemble beaucoup plus vaste de données qui du reste ne sont pas toujours confidentielles, étant entendu que, pour autant justement qu'elles y aient accès, les entreprises concurrentes peuvent éventuellement composer à partir de toutes ces données une mosaïque cohérente leur permettant d'en tirer des conclusions quant au développement et à la commercialisation du produit auquel ces

informations se rapportent. Les données – confidentielles – sur la base desquelles sont bâtis les dossiers d'autorisation des préparations originales (en vue de la protection du premier requérant), notamment, sont extrêmement coûteuses à établir. L'Institut Swissmedic a indiqué par ailleurs que cette affaire constituait à ses yeux un précédent, et qu'il s'attendait à ce que les demandes de consultation se multiplient, les entreprises pharmaceutiques voyant là un moyen d'accéder aux documents concernant des produits concurrents aux leurs. Il a également mis en avant le volume de travail énorme que ces demandes lui causaient, ainsi qu'aux entreprises pharmaceutiques qu'il avait l'obligation d'entendre. L'Institut Swissmedic a également évoqué la difficulté, s'agissant des pièces constitutives d'un dossier d'autorisation, qu'il avait à distinguer clairement entre ce qui relevait des données personnelles d'une part, et ce qui entrait dans le secret de fabrication et d'affaires d'autre part, les pièces concernées étant souvent situées à l'intersection des deux. Comme l'ont souligné les entreprises entendues, cela est particulièrement vrai lorsque le rapprochement – parfois à grands frais – d'informations par ailleurs déjà connues crée de la valeur, et justifie par conséquent de protéger l'accès à ces mêmes informations. Enfin, l'Institut Swissmedic a précisé:

- s'agissant de la demande en médiation déposée par les requérantes A et B: «que l'institut ne refusait pas l'accès aux documents conformément à l'accord signé en date du 2 juin 2009, mais qu'en vertu de la LTrans, l'institut avait consulté les personnes concernées, dans la mesure où les documents contiennent des données personnelles.»
- s'agissant de la demande en médiation déposée par les requérantes C, D et E: que les dispositions invoquées, à savoir l'art. 12 LPTH et l'art. 39, al. 3 de l'accord sur les ADPIC, n'étaient pas applicables dans le cas présent, car elles ne visaient pas directement à protéger les dossiers d'autorisation de préparations originales, mais réglaient les conditions dans lesquelles une demande d'autorisation déposée ultérieurement pouvait se référer à un tel dossier. À quoi s'ajoute qu'en tout état de cause, l'art. 39, al. 3 de l'accord sur les ADPIC n'est pas d'applicabilité directe.

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

1. A. Médiation et recommandation selon l'art. 14 LTrans

1. En vertu de l'art. 13 LTrans, toute personne peut déposer une demande en médiation auprès du Préposé fédéral à la protection des données et à la transparence lorsque sa demande d'accès à des documents officiels est limitée, différée ou refusée, ou lorsque l'autorité n'a pas pris position sur sa demande dans les délais. Peut également déposer une demande en médiation toute personne entendue selon l'art. 11, lorsque l'autorité entend accorder l'accès aux documents malgré son opposition.

   Le Préposé agit, non pas d'office, mais uniquement sur la base d'une demande[5]. Cette demande, qui doit clairement indiquer que l'affaire est confiée au préposé, doit être déposée par écrit dans un délai de 20 jours à compter de la réception de la prise de position de l'autorité.

2. Les requérantes A et B ont déposé une demande d'accès au sens de l'art. 10 LTrans auprès de l'Institut Swissmedic, qui leur a répondu par la négative. Etant parties à la procédure de demande d'accès, elles sont légitimées à déposer une demande en médiation, de même que les entreprises pharmaceutiques qui ont été entendues. Les demandes ont été remises au préposé en la forme (forme écrite simple) et dans les délais requis (soit dans un délai de 20 jours à compter de la réception de la prise de position de l'autorité).

3. La procédure de médiation peut se dérouler par écrit ou de vive voix (en présence de tous les intéressés ou de certains d'entre eux), sous l'égide du Préposé. Le Préposé fixe les modalités de la procédure[6].

   Si la médiation n'aboutit pas ou s'il est manifeste qu'aucune solution amiable ne pourra s'imposer, le préposé est tenu par l'art. 14 LTrans d'émettre une recommandation fondée sur son appréciation de l'affaire.

[5] FF 2003 1864
[6] FF 2003 1865

B. Champ d'application matériel

1. En vertu de l'art. 2, al. 1, let. a LTrans[7], la LTrans s'applique à toute l'administration fédérale, y compris à ses unités décentralisées. Or, l'Institut Swissmedic constitue une telle unité[8].

   L'Institut Swissmedic entre dans le champ d'application de la LTrans.

2. Les requérantes C et D ont notamment fait valoir que les art. 12 LPTh et 39, al. 3 de l'accord sur les ADPIC protégeaient les dossiers d'autorisation et interdisaient leur consultation.

   Il s'agit donc d'abord d'examiner si ces deux articles constituent des dispositions spéciales au sens de l'art. 4, let. a LTrans, ce qui entraînerait effectivement la non-applicabilité de la LTrans aux documents visés dans la présente affaire. Rappelons que l'art. 4 LTrans prévoit que sont réservées les dispositions spéciales d'autres lois fédérales qui déclarent certaines informations secrètes ou qui déclarent certaines informations accessibles, mais à des conditions dérogeant à la présente loi.

   Ni l'art. 12 LPTh, ni l'art. 39, al. 3 de l'accord sur les ADPIC ne visent directement le maintien du secret, pas plus qu'ils ne régissent la question de l'accès à l'information. Au surplus, l'art. 39, al. 3 de l'accord sur les ADPIC concerne les États membres et, n'étant donc pas d'applicabilité directe, il ne saurait fonder des prétentions de particuliers.

   Ces deux articles ne constituent donc pas des dispositions spéciales au sens de l'art. 4, let. a LTrans.

   Par ailleurs, il y a lieu d'examiner si les art. 61 (Obligation de garder le secret) et 62 (Confidentialité des données) LPTh constituent des dispositions spéciales au sens de l'art. 4 LTrans.L'obligation de garder le secret prévue à l'art. 61 LPTh ne régit que de manière très générale la confidentialité des données dans le domaine des produits thérapeutiques, et est assimilable au secret de fonction[9], qui n'entre

[7] FF 2003 1829
[8] Voir l'annexe de l'ordonnance sur l'organisation du gouvernement et de l'administration (RS 172.010.1) et FF 2003 1829
[9] FF 2003 1833

pas dans le champ d'application de l'art. 4 LTrans. Quant à l'art. 62 LPTh, le Conseil fédéral, dans sa réponse à la motion intitulée «Possibilité de consulter les dossiers relatifs à la procédure d'autorisation de médicaments», a précisé expressément qu'il «n'est pas non plus à considérer comme disposition législative spéciale régissant le droit d'accès visé à l'article 4 LTrans» [10].

Ni les art. 12 LPTH et 39, al. 3 de l'accord sur les ADPIC, ni les art 61 et 62 LPTh ne constituent des dispositions spéciales au sens de l'art. 4, let. a LTrans.

3. Est soumise à la LTrans toute information qui a été enregistrée sur un quelconque support (art. 5, al. 1, let. a LTrans) et qui est détenue par l'autorité dont elle émane ou à laquelle elle a été communiquée (art. 5, al. 1, let. b LTrans). Pour ce qui est des données qui font l'objet de la présente affaire, il s'agit, d'une part, des pièces et autres indications fournies à l'Institut Swissmedic par les entreprises pharmaceutiques pour lui permettre d'évaluer leur demandes d'autorisation de mise sur le marché d'un médicament ou d'un procédé (art. 10 et 11 LPTh), et d'autre part, des documents établis par l'Institut Swissmedic lui-même dans le cadre de la procédure d'autorisation. L'ensemble de ces données concernent l'accomplissement de la tâche publique dévolue à l'Institut Swissmedic.

   Toutes les pièces faisant partie des dossiers d'autorisation constituent des documents officiels au sens de l'art. 5, al. 1 LTrans et sont soumises à ce titre au principe de la transparence. Seule l'applicabilité d'une disposition des art. 7, 8 ou 9 LTrans pourrait légitimer une limitation du droit d'accès.

4. Un document officiel peut contenir des données personnelles, ou des informations constituant des «Exceptions» au sens de l'art. 7 LTrans (relevant par ex. du secret professionnel, du secret des affaires ou du secret de fabrication). Pour des raisons de méthode, on examinera d'abord la question de savoir si l'une desdites «Exceptions» est susceptible d'être invoquée, avant d'en venir à la question des données personnelles.

5. L'art. 7, al. 1, let. g LTrans permet de limiter ou de refuser le droit d'accès si l'accès peut «révéler des secrets professionnels, d'affaires ou de fabrication».

[10] Voir réponse du Conseil fédéral à la motion Teuscher 02.3748, qui précise notamment: «Le législateur ne part donc pas du principe que l'ensemble des informations rassemblées sur la base de la LPTh doit être traité de manière confidentielle. Il prévoit au contraire une solution permettant et exigeant une pesée des intérêts, comme celle qui est contenue dans le projet du Conseil fédéral pour une loi sur la transparence de l'administration (LTrans). L'article 62 LPTh n'est pas non plus à considérer comme disposition législative spéciale régissant le droit d'accès visé à l'article 4 LTrans. En cas d'introduction du principe de transparence, dans le sens du projet de loi du Conseil fédéral, le domaine des produits thérapeutiques ne serait pas pour autant soustrait au champ d'application de la LTrans.»

Du fait des obligations inhérentes à la procédure légale d'autorisation de mise sur le marché des médicaments, l'Institut Swissmedic s'est vu remettre par C, D et E un grand nombre d'informations qui figurent dans les dossiers d'autorisation. Or, ces informations ne sont pas nécessairement toutes confidentielles, ainsi celles que l'entreprise elle-même, ou une autre autorité (y compris une autorité étrangère, comme par ex. l'autorité de mise sur le marché européenne ou américaine), a déjà rendues publiques. Une divulgation ne risquant pas de nuire à l'entreprise concernée en permettant par ex. une utilisation abusive, ces informations doivent pouvoir être consultées.

L'exception visée à l'art. 7, al. 1, let. g LTrans protège uniquement les informations commerciales de C, D et E qui présentent effectivement un caractère confidentiel et que ces entreprises ont légitimement intérêt à voir garder confidentielles parce que leur divulgation serait la cause de distorsions de concurrence et, plus particulièrement, leur ferait perdre un avantage concurrentiel significatif. Dans les courriers qu'il a adressés à C, D et E (et notamment dans son courrier en date du 17 novembre 2009), l'Institut Swissmedic a d'ailleurs indiqué les passages qu'il convenait à ses yeux de caviarder au nom du secret de fabrication ou d'affaires.

Aux termes de l'art. 12, al. 1 OTrans, le Préposé examine si l'autorité a traité la demande d'accès d'une manière conforme à la loi et appropriée. Ainsi, le Préposé procède à la fois à un contrôle de l'application du droit, et, là où la loi laisse à l'autorité une certaine marge de manoeuvre (concernant par ex. le moyen qu'elle choisit pour rendre concrètement accessibles les documents officiels), à un contrôle du caractère adéquat de la solution retenue, compte tenu des caractéristiques particulières de chaque affaire. D'une façon générale, le Préposé juge conformes à la loi et appropriées la démarche suivie par l'Institut Swissmedic et la réponse qu'il a apportée à la question de savoir si les dossiers d'autorisation contenaient des informations couvertes par le secret de fabrication ou d'affaires et ce qu'il convenait en ce cas de faire.

6. Pour ce qui est de la question des données personnelles, celles-ci sont protégées par l'art. 9 LTrans.

Par données personnelles, on entend toutes les informations qui se rapportent à une personne identifiée ou identifiable (art. 3, let. a, de la loi fédérale sur la protection des données, LPD; RS 235.1). À cet égard, les documents officiels contenant des données personnelles doivent être si possible rendus anonymes avant qu'ils soient consultés (art. 9, al. 1 LTrans). Lorsque la demande d'accès porte sur des documents officiels qui ne peuvent pas être rendus anonymes, les dispositions régissant la communication de données personnelles par les organes fédéraux

s'applique (art. 9, al. 2 LTrans en rel. avec l'art. 19 LPD). L'art. 19, al. 1bis LPD autorise les organes fédéraux à communiquer des données personnelles en vertu de la LTrans si elles sont en rapport avec l'accomplissement de tâches publiques et si leur communication répond à un intérêt public prépondérant. Il constitue une disposition dite «de coordination» avec l'art. 7, al. 2 LTrans qui prévoit que le droit d'accès est limité si l'accès à un document officiel peut porter atteinte à la sphère privée de tiers. Ainsi, il peut arriver qu'un intérêt public à la transparence jugé prépondérant prime sur le respect de la sphère privée.

7. S'agissant des documents relatifs à la présente affaire, il est possible d'anonymiser certaines données personnelles. L'Institut Swissmedic l'a fait, et il a eu raison de le faire.

8. Cependant, il n'est pas possible d'anonymiser les informations qui concernent C, D et E. Aussi y a-t-il lieu de procéder à la confrontation des intérêts évoquée à l'art. 7, al. 2 LTrans. Dans le cadre de l'application de l'accord conclu avec les requérantes A et B suite aux audiences de médiation, l'Institut Swissmedic a entendu les entreprises C, D et E. À cette occasion, il leur a notamment rappelé le contenu et la finalité de la loi sur la transparence. Il leur a également indiqué son intention de faire droit aux demandes de consultation déposées par les requérantes A et B, et il leur a adressé copie des documents concernés après avoir marqué les passages qu'il entendait caviarder. Il les a également informés de la possibilité que leur offrait la loi de prendre position sur sa démarche. Une fois en possession des prises de position concernées, l'Institut Swissmedic a réexaminé la position qu'il avait arrêtée précédemment pour procéder à certains ajustements. Conformément à l'art. 11, al. 2 LTrans, l'Institut Swissmedic a informé C, D et E par lettre du 17 novembre 2009 des résultats de l'audition, en leur indiquant plus particulièrement qu'il avait conclu, après examen de chaque cas et compte tenu du principe de la proportionnalité, qu'en l'occurrence la sphère privée devait s'effacer devant un intérêt prépondérant de santé publique au sens de l'art. 6, al. 2, let. b OTrans et devant l'intérêt général du public à être informé au sens de la LTrans («dass der Beeinträchtigung der Privatsphäre ein überwiegendes Interesse der öffentlichen Gesundheit (vgl. Art. 6 Abs. 2 Bst. c [recte b] VBGÖ) und ein allgemeines Informationsinteresse gemäss BGÖ an der Einsichtnahme in ein Zulassungsdossier bzw. dessen Bearbeitung durch die Zulassungs- und Aufsichtsbehörde gegenüber [stehen].»). L'Institut Swissmedic a donc confirmé sa décision initiale d'accorder un accès partiel aux dossiers d'autorisation.

Le Préposé estime qu'en jugeant qu'un intérêt public justifiait qu'il soit donné partiellement accès à certains éléments des dossiers d'autorisation (art. 7, al. 2 LTrans, art. 9, al. 2 LTrans en rel. avec l'art. 19, al. 1bis LPD), l'Institut Swissmedic avait agi de manière conforme à la loi.

9. La présente affaire exigeait d'étudier un nombre de documents considérable (250 pages env.), et touchait à un domaine particulièrement complexe. Néanmoins, l'Institut Swissmedic a pris dûment en considération aussi bien les intérêts des entreprises pharmaceutiques concernées (et pour ce qui est de la sphère privée et pour ce qui est du secret de fabrication et d'affaires) que l'intérêt public à pouvoir consulter des documents officiels. En application du principe de la proportionnalité, l'Institut Swissmedic a décidé d'accorder un accès partiel aux dossiers d'autorisation, et il s'est expliqué de sa décision auprès des entreprises concernées, notamment dans son courrier du 17 novembre 2009. Enfin, le Préposé constate que tout au long de la procédure, et singulièrement depuis que se sont déroulées les deux audiences de médiation, l'Institut Swissmedic a accordé un prix particulier à la loi sur la transparence et à son objet.

   Le Préposé estime adaptée au cas particulier la démarche adoptée par l'Institut Swissmedic, et appropriée sa décision d'autoriser un accès partiel aux dossiers.

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

1. L'institut Swissmedic accorde partiellement l'accès aux dossiers d'autorisation de mise sur le marché des médicaments produits par C, D et E, conformément à ce qu'il avait déjà indiqué dans son avis en date du 17 novembre 2009.

2. Si l'Institut Swissmedic refuse d'accorder l'accès aux dossiers d'autorisation et s'oppose donc à la recommandation émise au point 1, il rend une décision au sens de l'art. 5 de la loi sur la procédure administrative (PA, RS 172.021).

   L'Institut Swissmedic rend sa décision dans un délai de vingt jours à compter de la réception de la présente recommandation (art. 15, al. 3 LTrans).

3. Si les requérants rejettent la présente recommandation, ils peuvent, dans un délai de dix jours à compter de la réception de la présente recommandation, demander à l'Institut Swissmedic de rendre une décision au sens de l'art. 5 PA (art. 15, al. 1 LTrans).

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

5. La présente recommandation est publiée. Afin de protéger les données personnelles des parties à la procédure de médiation, les noms des demandeurs ont été anonymisés (art. 13 OTrans).

6. Par analogie à l'art. 22a de la loi fédérale sur la procédure administrative (RS 172.021), les délais fixés en jours par la loi ne courent pas du 7e jour avant Pâques au 7e jour après Pâques inclusivement. Le délai débute donc le 12 avril 2010.

7. La présente recommandation est notifiée:

   - A (recommandation en allemand et traduction en français)
   - B (recommandation en allemand et traduction en français)
   - C
   - D
   - E
   - Swissmedic (recommandation en allemand et traduction en français)

     Hallerstrasse 7

     Postfach

     3000 Bern 9

Hanspeter Thür

4.2.4 Recommandation adressée à l'Office fédéral de la justice: «Loterie Romande»

Berne, le 28 avril 2010

Recommandation

émise au titre

de l'art. 14
de la loi fédérale
sur le principe de la transparence
dans l'administration

concernant la demande en médiation introduite

par X
(demandeur)

contre

l'Office fédéral de la justice

I. Le Préposé fédéral à la protection des données et à la transparence constate les faits suivants:

1. Le demandeur (personne privée) a déposé le 12 février 2010 auprès de l'Office fédéral de la justice (OFJ) une demande d'accès aux «chiffres des billets 'non vendus' de la Loterie Romande» de l'année 2008.

2. Le 15 février 2010, l'OFJ a répondu au demandeur que «Le nombre de billets non vendus en 2008 par la LoRo [Loterie Romande] ne nous a malheureusement pas été fourni. Nous vous prions donc de vous adresser directement auprès de la LoRo.»

3. Dans son courriel de réponse du 15 février 2010, le demandeur a constaté que selon l'article 5 de l'Ordonnance relative à la loi fédérale sur les loteries et les paris professionnels (OLLP), le nombre des billets non vendus ainsi que d'autres indications devaient être en possession de l'OFJ. Selon cette disposition, l'office était tenu de dresser un tableau sur la base de ces indications et devait le publier d'une manière appropriée.

4. Par courriel du 22 février 2010, l'OFJ a répondu au demandeur que l'office «dispose d'une certaine marge de manœuvre pour la publication de ces données.» En outre, l'OFJ a précisé que «les billets non vendus, les délais d'exploitation, le nombre des lots… ne présentent pas, de notre point de vue, d'intérêt suffisant pour que nous exigions de recevoir des données. Par habitude, nous publions les indications sur le montant des billets non vendus si les chiffres nous en sont fournis.»

5. Par courrier du 24 février 2010, le demandeur a exigé de l'OFJ de bien vouloir veiller, en tant qu'Autorité fédérale, [à] la bonne application de l'art. 5 OLLP comme prévu par la Loi fédérale, et non comme voulu par la Loterie Romande. En cas de refus de votre part de faire respecter l'art. 5 OLLP comme demandé, je vous prie de bien vouloir me faire connaître la voie de recours à suivre pour contester votre décision.»

6. Par lettre du 10 mars 2010, l'OFJ a informé le demandeur entre autres de la possibilité d'exiger une décision de non-entrée en matière contre laquelle il pouvait recourir au Tribunal administratif fédéral.

7. Le 22 mars 2010, le demandeur a déposé auprès du Préposé fédéral à la protection des données et à la transparence (ci-après: Préposé) une demande en médiation selon l'art. 13 de la loi fédérale sur le principe de la transparence dans l'administration (loi sur la transparence, LTrans; RS 152.3).

8. A la demande du Préposé, l'OFJ lui a transmis les données statistiques communiquées par le canton de Vaud et la Loterie Romande ainsi qu'un extrait du système de gestion des documents de l'unité compétente de l'OFJ. L'OFJ a confirmé dans sa prise de position qu'il ne détenait pas d'information concernant le nombre de billets non vendus en 2008 par la Loterie Romande.

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

A. Médiation et recommandation selon l'art. 14 LTrans

1. En vertu de l'art. 13 LTrans, toute personne peut déposer une demande en médiation lorsque sa demande d'accès à des documents officiels est limitée, différée ou

refusée, ou lorsque l'autorité n'a pas pris position sur sa demande dans les délais requis.

Le Préposé n'agit pas d'office, mais seulement sur la base d'une demande déposée par écrit[1]. Toute personne qui a pris part à une procédure de demande d'accès à des documents officiels est habilitée à introduire une demande en médiation. Pour adresser une demande en médiation, la forme écrite simple suffit. La demande doit spécifier que l'affaire est confiée au Préposé. Elle doit être déposée dans les 20 jours à compter de la réception de la prise de position de l'autorité.

2. Le demandeur a déposé une demande d'accès au sens de l'art. 10 LTrans auprès de l'OFJ et a reçu une réponse négative. Etant partie à la procédure de demande d'accès, il est légitimé à déposer une demande en médiation. Celle-ci a été déposée auprès du Préposé par écrit dans le délai requis.

3. La procédure de médiation peut se dérouler par écrit ou de par oral (en présence de tous les intéressés ou de certains d'entre eux), sous l'égide du Préposé. C'est à lui qu'il incombe d'en fixer les modalités[2].

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

B. Champ d'application matériel

1. La loi sur la transparence s'applique uniquement à des documents qui sont détenus par l'autorité dont ils émanent ou à laquelle ils ont été communiqués (art. 5 LTrans). Le message relatif à la loi précise clairement que «le principe de transparence *ne saurait* contraindre l'administration à établir un document qui n'existe pas.» En d'autres mots, le demandeur ne peut pas exiger *sur la base* de la loi sur la transparence que l'OFJ établisse un document.

2. La loi sur la transparence régit l'accès à des documents officiels requis par un demandeur. Il s'agit d'un cas d'application d'information dite passive. Il se distingue de l'information active qui est régie par des dispositions légales spéciales qui obligent l'autorité à publier certaines informations.

   Même si une autorité est tenue d'informer activement sur la base d'une disposition légale spécifique, la loi sur la transparence ne confère au demandeur aucun droit à obtenir la publication de l'information en question.

[1] FF 2003 1864
[2] FF 2003 1865

3. L'OFJ a soumis au Préposé un extrait de son système de gestion des documents ainsi que les données statistiques communiquées par le canton de Vaud et la Loterie Romande. Le Prépose n'a aucune raison de douter de la vraisemblance et du sérieux des allégations de l'OFJ concernant le fait que cet office ne détient pas d'information concernant le nombre de billets non vendus en 2008 par la Loterie Romande.

III. Se fondant sur les considérations susmentionnées, le Préposé fédéral à la protection des données et à la transparence recommande:

1. Vu que l'Office fédéral de la justice ne détient pas les informations requises par le demandeur, il n'est pas tenu d'établir un tel document sur la base de la loi sur transparence.
2. Dans les dix jours à compter de la réception de la recommandation, le demandeur peut exiger que l'Office fédéral de la justice rende une décision selon l'art. 5 de la loi fédérale sur la procédure administrative (PA, RS 172.021) s'il n'est pas d'accord avec la recommandation (art. 15, al. 1, LTrans).
3. La décision peut faire l'objet d'un recours devant le Tribunal administratif fédéral (art. 16 LTrans).
4. La présente recommandation est publiée (art. 13, al. 3, de l'ordonnance sur la transparence, OTrans; RS 152.31). Le nom du demandeur a été anonymisé afin de protéger les données relatives aux parties à la procédure de médiation.
5. La recommandation est notifiée:
   - à X
   - à l'Office fédéral de la justice

     3003 Berne

Hanspeter Thür

4.2.5 Recommandation adressée au Département de la défense, de la protection de la population et des sports: «Imams islamistes»

Voir chiffre 4.2.5 de la partie en langue allemande

4.2.6 Recommandation adressée à l'Office fédéral de l'agriculture: «Groupe de travail constitué par le Département fédéral de l'économie»

Voir chiffre 4.2.6 de la partie en langue allemande