12ème Rapport d'activités 2004/2005

Préposé fédéral à protection des données

Rapport d'activités 2004/2005 du Préposé fédéral à la protection des données

Le Préposé fédéral à la protection des données est tenu de fournir périodiquement au Conseil fédéral un rapport sur son activité (article 30 de la loi fédérale sur la protection des données). Le présent rapport couvre la période du 1er avril 2004 au 31 mars 2005.

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

Distribution:

OFCL, Vente des publications fédérales, CH-3003 Berne

www.bbl.admin.ch/bundespublikationen

No d'art. 410.012.d/f

Table des matières

* Version originale en allemand

* Version originale en allemand

* Version originale en allemand

Avant-propos

«L'occasion fait le larron», dit le proverbe. Dans le contexte de la protection des données, on pourrait dire: toute nouvelle banque de données éveille l'appétit de nouvelles utilisations. Où est le problème?

Le risque existe que d'importants principes de la loi sur la protection des données soient balayés. Prenons pour exemple le principe de finalité. Ce principe important exige que les données collectées ne soient utilisées que dans le but pour lequel elles ont été rassemblées à l'origine. Par exemple, le patient qui confie ses maux à son médecin n'est pas obligé d'accepter que son adresse soit transmise, sans son consentement, à une entreprise pharmaceutique produisant les médicaments dont il a besoin.

Bien que ce principe semble aller de soi, dans la pratique, l'appétit de données éveillé par la création de nouvelles banques de données ne peut pas toujours être écarté, et les abus ne peuvent pas toujours être évités. Ainsi les cartes-clients des grands distributeurs commerciaux intéressent régulièrement toutes sortes d'autorités. Où se situe la frontière entre ce qui est autorisé et ce qui ne l'est pas? Il est incontesté que dans le cadre d'une procédure pénale, le nom du titulaire d'une carte peut être dévoilé. La protection des données ne saurait protéger les délinquants. Par contre, la situation devient délicate lorsque, par exemple, l'Administration fédérale des contributions – comme cela s'est produit récemment – demande à un grand distributeur toutes les données concernant un client dans une affaire relative à la taxe à la valeur ajoutée. Précisons à ce propos que ces informations ne disaient que très peu de choses sur les habitudes d'achat effectives du titulaire de la carte. En effet, une carte-client peut être utilisée de manière très sélective ou encore par plusieurs personnes. Dans ce cas, le distributeur a bien fait de refuser de transmettre les données en question. S'il avait agi autrement, il aurait contrevenu à la loi sur la protection des données.

Ces exemples donnent à penser qu'à l'avenir, l'appétit de données des autorités ne fera que croître, tout comme le besoin de puiser des données dans toutes sortes de fichiers existants. Voyons ce qu'il se passe à l'étranger: En Allemagne par exemple, une loi est entrée en vigueur sans faire de bruit; celle-ci permet à un grand nombre d'autorités administratives (offices des finances, des bourses d'études, des affaires sociales, du logement) d'avoir accès aux comptes privés de chaque citoyenne ou citoyen. Pour un tel accès généralisé à cet aspect de la sphère privée du citoyen, un soupçon de comportement malhonnête n'est même pas nécessaire. Il sera intéressant de voir comment la Cour constitutionnelle allemande réagira aux plaintes déposées dernièrement par deux citoyens.

Aux Etats-Unis, l'échange de données entre les entreprises privées et l'Etat est déjà considérable. Un rapport du General Accounting Office (une commission de gestion) montre que des entreprises privées (par ex. les éditeurs de cartes de crédit et les agences de renseignements sur les crédits) fournissent des données à l'Etat dans le cadre de nombreux projets. L'Union américaine des libertés civiles constate avec inquiétude que des sociétés privées (banques, compagnies d'aviation, sociétés de cartes de crédit, agences de location de voitures, etc.) sont de plus en plus nombreuses à vendre leurs fichiers de données-clients au gouvernement. De nombreux vendeurs professionnels de listes d'adresses travaillant à grande échelle – seraient actuellement en mesure de fournir des listes de personnes qui, par exemple, prennent un médicament contre la dépression, croient en la bible, jouent en ligne ou achètent des accessoires érotiques. Cette tendance s'est très fortement accrue avec la lutte contre le terrorisme: le Patriot Act américain oblige désormais certaines entreprises privées à fournir des données.

Même des lois clairement formulées ne permettent pas de garantir l'absence d'abus: La nouvelle loi sur les péages (Mautgesetz), une loi qui ne permet le traitement des données collectées que dans des buts spécifiques, était à peine introduite en Allemagne que les autorités de poursuite pénale demandaient les données recueillies afin de sanctionner les dépassements de vitesse. Ce n'est que grâce à l'intervention du préposé fédéral allemand à la protection des données que le législateur a clairement établi que toute transmission, utilisation ou saisie de données en vertu d'autres dispositions légales était illicite. Mais qu'adviendra-t-il si le législateur change d'avis dans quelques années?

La Suisse aussi est concernée. D'une part, l'expérience nous a appris que ce genre d'évolution à l'étranger laisse également des traces en Suisse. Chez nous également, les nouvelles banques de données éveillent de nouveaux besoins: des fichiers constitués sont utilisés dans bien d'autres buts que celui poursuivi à l'origine. Leurs possibilités d'utilisation deviennent plus larges en raison de techniques de traitement plus pointues. D'autre part, ce qu'il se passe au-delà de nos frontières nous sensibilise aux problèmes pouvant surgir chez nous dans le cadre des échanges de données internationaux. La question très concrète qui se pose toujours est de savoir si un niveau suffisant de protection des données est garanti dans le pays concerné et si la transmission de données peut se faire sans crainte.

D'une manière plus générale, on peut se demander si face à ce genre d'évolution, la sphère privée a encore vocation d'exister. Les voix qui prétendent le contraire ne sont pas nouvelles. David Brin, par exemple, a développé dans son essai «The transparent Society» la vision d'une société dans laquelle tout le monde peut surveiller tout le monde et est autorisé à le faire. La multiplication des cybercaméras privées ainsi que des caméras vidéo installées dans de nombreux bistrots et discothèques qui retransmettent en direct leurs images sur le réseau Internet, montre à l'évidence que beaucoup de personnes ne sont pas dérangées par le fait de se savoir surveillées. La mentalité du «Je n'ai rien à cacher» pourrait légitimer la création d'une banque de données d'ADN qui nous engloberait tous. La présomption d'innocence, principe central dans un Etat démocratique est dans ces conditions sérieusement mise à mal.

On a parfois l'impression que les civilisations occidentales – qui devaient leur rayonnement à l'esprit libéral et éclairé de leurs pères fondateurs, et de ce fait réputées supérieures aux régimes communistes autoritaires auxquels elles ont survécu sont fatiguées de défendre les libertés publiques. De plus en plus, notre société cherche le salut dans un contrôle et une surveillance toujours plus grands. Or quiconque ne défend plus les libertés et droits fondamentaux – et la protection de la sphère privée en fait partie – n'en est plus digne!

Enfin, il nous est démontré qu'en matière de protection des données également, les solutions sur le plan strictement national ne mènent pas au but. Dans un monde globalisé aux flux de données globales, l'élaboration de normes de protection des données de portée internationale revêt une importance majeure.

Ce sera également l'objectif principal de la 27ème Conférence Internationale des Commissaires à la protection des données qui se réunira cette année pour la première fois en Suisse (à Montreux, du 14 au 16 septembre). Le Préposé fédéral à la protection des données est très heureux d'accueillir cette rencontre. Nous nous sommes attelés à notre tâche avec une grande motivation et un grand esprit d'engagement. Placée sous le thème de « La protection des données personnelles et de la sphère privée dans un monde globalisé », cette conférence nous permettra justement de nous interroger justement à ce propos. Dix ans exactement après la mise sur pied de la directive de l'Union européenne 95/46/CE «relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données», nous aimerions tirer un bilan. La directive a-t-elle apporté ce que l'on attendait d'elle? Quel écho rencontre-t-elle aujourd'hui dans le contexte international? Faut-il une nouvelle initiative au niveau mondial pour dynamiser et unifier la protection des données? Nous adopterons, à l'occasion de cette conférence, une déclaration finale qui tentera de répondre à ces questions.

Répertoire des abréviations

AVRE	Ambient Voice Recording
BEAA	Bureau d'enquête sur les accidents d'aviation
CFPD	Commission fédérale de la protection des données
CNA	Caisse nationale suisse d'assurance en cas d'accidents
CP	Code pénal
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
DPS	Détection et suivi des personnes atteintes dans leur santé
EAN	European Article Number
EPC	Electronic Product Code
IMES	Office fédéral de l'immigration, de l'intégration et de l'émigration (actu ellement Office fédéral des migrations, OFM)
LAA	Loi fédérale sur l'assurance-accidents
LAGH	Loi fédérale sur l'analyse génétique humaine
LAMal	Loi fédérale sur l'assurance-maladie
LBA	Loi sur le blanchiment d'argent
LCA	Loi fédérale sur le contrat d'assurance
LMSI	Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure
LOC	Loi fédérale sur les Offices centraux de police criminelle de la Confédération
LPD	Loi fédérale sur la protection des données
LSA	Loi fédérale sur la surveillance des assurances
METAS	Office fédéral de métrologie et d'accréditation

OALSP	Ordonnance du 14 juin 1993 concernant les autorisations de lever le secret professionnel en matière de recherche médicale
OBCBA	Ordonnance sur le Bureau de communication en matière de blanchiment d'argent
ODR	Office fédéral des réfugiés (actuellement Office fédéral des migrations, OFM)
OFAC	Office fédéral de l'aviation civile
OFAS	Office fédéral des assurances sociales
OFJ	Office fédéral de la justice
OFP	Office fédéral de la police (actuellement fedpol)
OFS	Office fédéral de la statistique
PFPD	Préposé fédéral à la protection des données
RFID	Radio Frequency Identification
SAS	Service suisse d'accréditation
SIS	Système d'information de Schengen
WPISP	Working Party for Information Security and Privacy
ZIS	Système central d'information

1 Droits fondamentaux

1.1 Modernisation de la protection des données

1.1.1 Révision de la loi fédérale sur la protection des données

En réponse à deux motions parlementaires, le Conseil fédéral a adressé aux Chambres fédérales le 19 février 2003 le message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Ces projets sont en cours d'examen au Parlement fédéral.

En réponse à la motion 98.3529 de la Commission de gestion du Conseil des Etats «liaisons on-line: renforcer la protection pour les données personnelles» et à la motion 00.3000 de la Commission des affaires juridiques du Conseil des Etats «renforcement de la transparence lors de la collecte des données personnelles», le Conseil fédéral a adressé aux Chambres fédérales le 19 février 2003 le message relatif à la révision de la loi fédérale sur la protection des données (LPD) et à l'arrêté fédéral concernant l'adhésion de la Suisse au Protocole additionnel du 8 novembre 2001 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel concernant les autorités de contrôle et les flux transfrontières de données (FF 2003 1915) (voir aussi 10ème rapport d'activités 2002/2003, chiffre 1.1). Lors de la session de printemps 2004, le Conseil national a accepté d'entrer en matière sur ce projet. Il a toutefois décidé de renvoyer le dossier au Conseil fédéral en le chargeant de préparer un projet moins ambitieux. La majorité du Conseil était en effet d'avis que le projet du Conseil fédéral allait au-delà de l'objectif des deux motions. Elle souhaitait que l'on s'en tienne aux motions et aux modifications nécessaires à la ratification du protocole additionnel. Le Conseil des Etats n'a pas suivi le Conseil national et a estimé que le projet présenté par le Conseil fédéral pouvait être traité par les commissions compétentes. Finalement, le Conseil national s'est rallié et la commission des affaires juridiques va reprendre le dossier. Nous nous réjouissons de cette décision qui évite de retarder l'adoption de ce projet. Nous soutenons dans l'ensemble le projet de révision de la LPD et la ratification du protocole additionnel. Nous aurions souhaité une révision plus étendue et notamment un rapprochement plus conséquent avec le droit européen. Nous estimons cependant qu'il est préférable d'agir par étapes. Le projet du Conseil fédéral est la réponse aux deux motions précitées et le préalable indispensable à la ratification du protocole additionnel. Le projet se limite à

l'essentiel. La plupart des propositions sont la conséquence directe de la réalisation des deux motions (transparence, droit des personnes concernées, registre des fichiers, surveillance du PFPD, traitement sur mandat, etc.) ou de la ratification du protocole additionnel (flux transfrontières de données, droit de recours du PFPD, surveillance du PFPD). La révision tient largement compte de la procédure de consultation. En particulier, nous saluons l'introduction de la certification et du label de qualité de protection des données qui permettra de renforcer l'autonomie et la responsabilité des maîtres de fichier et d'encourager l'autoréglementation. Nous maintenons cependant nos réserves concernant la réglementation des projets-pilotes. Nous espérons que les débats permettront de revoir cette question.

Parmi les critiques adressées au projet figure l'obligation d'information. On craint que cette obligation n'aille trop loin et provoque une charge administrative supplémentaire. Ainsi que l'exige la motion de la Commission des affaires juridiques du Conseil des Etats, le projet de loi prévoit une obligation détaillée d'informer lors de la collecte de données sensibles ou de profils de la personnalité. En outre, le projet de loi prévoit en outre que la collecte de données personnelles et les finalités du traitement doivent être reconnaissables pour la personne concernée. Cette disposition concrétise le principe de la bonne foi et reflète l'intérêt des personnes concernées à l'existence d'un minimum de transparence lors de la collecte de données non sensibles. Le coût de la transparence ne doit pas être exagéré. Le principe de proportionnalité s'applique également dans ce contexte. Ainsi, une information détaillée n'est pas nécessaire lors de chaque collecte de données. La forme et le contenu de l'information vont dépendre de différents critères, en particulier du but, des méthodes et des circonstances du traitement, ainsi que de l'information dont dispose déjà la personne concernée. L'information peut être donnée de manière générale (publication, Internet, conditions générales, information standardisée, etc.). Plusieurs entreprises respectent aujourd'hui déjà le principe de transparence. La transparence est non seulement dans l'intérêt de la personne concernée, mais également dans l'intérêt de l'économie. Le Parlement a déjà reconnu le besoin de transparence dans d'autres domaines, par exemple dans le cadre de la révision de la loi fédérale sur le contrat d'assurances qui prévoit un devoir d'information plus large pour le traitement de données personnelles. Nous ne pouvons pas suivre les critiques selon lesquelles l'obligation d'information coûterait trop cher et que de toute façon les personnes concernées ne seraient pas intéressées à leurs données, du fait que très peu d'entre elles feraient usage de leur droit d'accès. En effet, nous recevons quotidiennement des demandes de citoyens qui s'informent de leurs droits et qui souhaitent recevoir des informations sur les traitements les concernant. Le citoyen ignore souvent qui traite des données à son sujet et quels sont ses droits. Il a souvent trop de respect à l'égard des maîtres de fichier. Il hésite à introduire

une procédure pouvant s'avérer contraignante. Dans d'autres Etats dotés d'une loi de protection des données équivalente, le principe de transparence est également reconnu. Dans ces pays, l'obligation d'informer est bien acceptée par les responsables de traitement et n'est plus sujette à discussions. Pour l'économie et les entreprises, il est également plus avantageux d'avoir affaire à des clients informés. La transparence permet également de renforcer la confiance entre les entreprises et leurs clients.

Un autre point du projet de révision est l'objet de critiques, à savoir celui des compétences de surveillance du PFPD dans le secteur privé. On craint qu'il n'intervienne dans chaque cas d'espèce. D'une part, une telle interprétation serait contraire à l'esprit et à la lettre de la disposition proposée. D'autre part, le PFPD n'a pas les ressources nécessaires pour s'occuper de chaque cas d'espèce. Les modifications proposées allègent la procédure d'annonce des fichiers. Elles ne créent pas de nouvelles compétences. Actuellement, le PFPD peut déjà intervenir lors de traitements de données sensibles ou de profils de la personnalité. En effet, l'individu n'est souvent pas en mesure d'introduire une procédure, faute de moyens. Le PFPD doit ainsi avoir la possibilité d'intervenir dans les cas qui comportent un risque particulier d'atteinte aux droits de la personnalité. Les traitements de données sensibles ou de profils de la personnalité qui touchent un grand nombre de personnes constituent de tels cas.

1.1.2 Procédure de certification proposée dans la révision partielle en cours de la loi fédérale sur la protection des données.

Afin d'introduire une autoréglementation renforçant la responsabilité du maître de fichier et stimulant la concurrence, une procédure de certification est prévue dans la nouvelle LPD pour les organisations aussi bien que pour les produits. L'ordonnance relative à la LPD révisée par l'Office fédéral de la Justice devrait contenir les conditions essentielles auxquelles les organismes de certification seront soumis, en accord avec le Service suisse d'accréditation. Parallèlement, un cadre standard d'évaluation du niveau requis de protection des données est en cours d'élaboration par le PFPD, afin de spécifier les exigences minimales d'un système de gestion de la protection des données.

En collaboration avec l'Office fédéral de la Justice (OFJ) qui est responsable de la révision partielle de la LPD, nous avons examiné les prochaines étapes nécessaires à la concrétisation de la «procédure de certification». La révision de la LPD devrait permettre d'introduire le principe de l'autoréglementation, afin de renforcer la responsabilité du maître de fichier et de stimuler la concurrence et d'améliorer ainsi la protection et la sécurité des données. Même si le projet vise à encourager les procédures de certification aussi bien des structures d'organisation et processus d'exploitation que des systèmes techniques d'information ou programmes (c'est-à-dire de produits), l'accent devrait être mis en premier lieu sur la certification d'organisations, pour laquelle l'attrait escompté semble plus important. Dans le cadre des travaux préparatoires de révision de l'ordonnance relative à la LPD, des discussions sont en cours pour y introduire les conditions essentielles auxquelles les organismes de certification seront soumis, et ce en collaboration étroite avec le Service suisse d'accréditation (SAS) de l'Office fédéral de métrologie et d'accréditation (METAS). En ce qui concerne les aspects plus spécifiques et pratiques de la procédure de certification proprement dite, à savoir un cadre standard d'évaluation du niveau de protection des données, nous examinons l'opportunité de la mise en place d'un référentiel-modèle. Ce dernier pourrait se baser sur la norme d'audit BS 7799-2:2002 avec ses spécifications pour les systèmes de gestion de la sécurité de l'information (SGSI), prenant elle-même appui sur la norme internationale ISO 17799:2000 avec son code de pratique (CdP: 10 chapitres comprenant non moins de 128 contrôles) pour la gestion de la sécurité de l'information. Dans le cadre du système de gestion de la protection des données (SGPD) envisagé, l'accent devrait être mis sur les principes et méthodes garantissant ou améliorant la protection des données, y compris ceux et celles provenant de modèles ou référentiels utilisés par des instances nationales ou internationales impliquées dans des démarches similaires.

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

Les autorités américaines offrent à la Suisse les mêmes garanties en matière de protection des données que celles accordées à l'Union européenne. Ces garanties, contenues actuellement dans une note diplomatique, doivent figurer dans un accord bilatéral. Les passagers sont informés que des données les concernant sont transmises aux autorités américaines. Les autorités canadiennes offrent également à la Suisse les mêmes garanties que celles accordées à l'Union européenne. Celles-ci sont quant à elles mentionnées dans un accord bilatéral.

Dans notre 11ème rapport d'activités 2003/2004 (chiffre 1.1.2), nous avons mentionné que les autorités suisses avaient décidé d'engager des négociations avec les autorités américaines afin d'élaborer un accord bilatéral relatif au transfert de données personnelles permettant d'assurer les liaisons aériennes avec les Etats-Unis tout en respectant les principes généraux de protection des données. Dans le cadre de ces négociations, les autorités américaines ont offert à la Suisse les mêmes garanties en matière de protection des données que celles accordées à l'Union européenne. Ces garanties figurent dans un accord entre la Commission européenne et le gouvernement américain. En ce qui concerne notre pays, les autorités américaines proposent un échange de notes diplomatiques. Une telle base légale est insuffisante au regard de la LPD. Cependant, le groupe de travail interdépartemental, auquel nous participons, estime que la proposition des Etats-Unis permet de réduire notoirement les atteintes à la personnalité des passagers. En effet, les données sont transmises par les compagnies aériennes et les autorités américaines n'ont pas d'accès aux systèmes de réservation. Les données sensibles comme les soins médicaux ou les repas choisis à bord ne sont pas transmises aux Etats-Unis. Les données communiquées sont uniquement utilisées pour prévenir et combattre le terrorisme, les crimes liés au terrorisme ainsi que d'autres crimes graves, notamment la criminalité organisée. La conservation des données est limitée à trois ans et demi. Les personnes résidant en Suisse peuvent directement ou par l'intermédiaire du PFPD faire valoir leurs droits aux Etats-Unis. Enfin, le respect des garanties fournies est contrôlé une fois par an par les autorités des deux pays. Les passagers sont dans tous les cas informés avant de monter à bord de l'avion que des données personnelles sont transmises aux autorités américaines. Dans le cadre de notre participation au groupe de travail interdépartemental, nous soutiendrons toujours la position selon laquelle un accord bilatéral avec les Etats-Unis donnant un cadre légal suffisant à ces communications doit être élaboré.

Les autorités canadiennes ont offert les mêmes garanties que celles accordées à l'Union européenne. Le Canada est aussi prêt à conclure un accord bilatéral avec la Suisse. Il y a lieu également de préciser que, contrairement aux Etats-Unis, le Canada dispose d'une législation sur la protection des données équivalente à la législation suisse.

1.2 Autres thèmes

1.2.1 Identificateur et registre de personnes

La Confédération, les cantons et les communes enregistrent des données personnelles dans différents registres. Dans le cadre de l'harmonisation des registres de personnes, différents travaux ont été entrepris en Suisse depuis plusieurs années déjà pour introduire un identificateur de personne qui devrait permettre de relier entre eux les registres existants. Les conséquences de l'identificateur de personne n'ont jusqu'à ce jour pas été suffisamment analysées, ni discutées sur le plan politique. Nous avons relevé à plusieurs reprises que les processus et opérations devant être facilités par l'identificateur de personne devaient être définis et analysés de manière précise afin de permettre une réflexion sur la sécurité et la protection des données.

L'identificateur de personne comme nouveau moyen permettant de relier entre eux les principaux registres administratifs de personnes de notre pays est, en particulier dans le cadre de différentes procédures de consultation, un sujet constant de notre attention. C'est dans le cadre de l'harmonisation des registres de personnes – un projet soutenu par l'Office fédéral de la statistique (OFS) en prévision du recensement de la population de 2010 – que les travaux visant à faciliter et à automatiser la mise en relation d'inscriptions de différents registres de personnes ont été lancés pour la première fois. Il était évident dès le début que ces travaux soulèveraient des problèmes au niveau de la protection des données, ceci pour deux raisons. D'une part, tous ces travaux ont été effectués en partant de l'hypothèse qu'un identificateur de personne serait introduit dans les registres administratifs de personnes pour permettre la mise en relation. D'autre part, les modèles de base pour une harmonisation des registres ont été élaborés sans prendre en compte les aspects de la protection de la personnalité.

Dans nos premières prises de position en 2001, nous avions déjà informé l'OFS qu'il n'était pas admissible d'introduire de nouveaux attributs d'identification dans les registres administratifs à des fins statistiques. Nous avions recommandé de recourir plutôt à des modèles utilisant des pseudonymes ou à des méthodes telles que celles qui ont déjà fait leurs preuves dans le domaine de la statistique médicale des hôpitaux. Comme toutes nos autres remarques, cette suggestion n'a pas été prise en compte dans le projet d'harmonisation des registres.

Entre-temps, le projet «identificateur de personne» a été formellement séparé du projet d'harmonisation des registres. Les deux projets restent cependant étroitement liés au niveau de leurs contenus, ainsi qu'au niveau de la pression du temps imposée en prévision du recensement de 2010 qui approche à grands pas.

Le projet présenté au printemps 2004 par l'OFS prétendait résoudre les problèmes liés à la protection des données au moyen d'identificateurs de personne appelés «sectoriels». En fait, les six secteurs mentionnés dans ce projet n'existent pas dans la réalité pratique de l'administration. Il n'est d'ailleurs pas envisageable que l'on crée de tels secteurs, isolés les uns des autres. Une des raisons est que la plupart des registres de personnes sont tenus selon les dispositions légales des cantons et communes qui les gèrent et qu'il n'est donc pas réaliste d'admettre que la Confédération puisse leur demander de dissocier ces registres alors que l'on parle d'«harmonisation des registres». Il est donc évident que la sectorialisation n'est pas vraiment apte à résoudre les problèmes liés à la protection des données; il n'est pas étonnant non plus que les identificateurs sectoriels de personne n'aient pas rencontré un écho favorable lors de la procédure de consultation et qu'ils aient entre-temps à nouveau été retirés du projet.

Nous avons fait parvenir à l'OFS deux prises de position concernant le projet précité qui, à l'exception des remarques relatives aux secteurs, sont toujours valables. Dans ces prises de position, nous avons notamment critiqué le fait que même la version actuelle du projet (le moyen de liaison prévu s'appelle maintenant «identificateur personnel du secteur population») ne contient aucune réflexion sur les risques engendrés par l'interconnexion des registres et la mise en réseau électronique. Il semble que l'on parte du principe qu'il n'y aurait pas de risque en matière de protection des données, puisque l'objectif recherché consisterait uniquement à «automatiser les processus de communication de données existants prévus par la loi». Cette interprétation ne tient cependant pas compte de la différence fondamentale qui existe entre le monde traditionnel du document papier et le monde électronique. En effet, s'il s'agissait réelle-

ment d'éviter de nouveaux flux de données, il conviendrait d'abord, avant l'automatisation, de dissocier de manière stricte tous les registres cantonaux concernés selon les dispositions fédérales. Il ne serait par exemple pas acceptable qu'un canton tienne son registre des habitants dans le même fichier que d'autres registres.

Au niveau des bases légales et constitutionnelles, nous avons en substance critiqué trois points: Premièrement, on peut se demander si un identificateur de personne créé à des fins statistiques (et reposant sur une base constitutionnelle suffisante) peut également être utilisé à des fins administratives. A notre avis, une nouvelle compétence est ainsi attribuée à la Confédération, ce qui implique de la nécessité de créer une base légale constitutionnelle. En effet, les projets présentés créeraient tout de même un registre virtuel comprenant tous les habitants de la Suisse. Un deuxième point que nous critiquons est le fait que les projets élaborés jusqu'ici ne respectent pas le principe de la légalité, les bases légales n'étant en effet pas suffisamment concrètes. Or, il est inadmissible de renoncer à procéder à l'analyse et à la description des processus et des opérations devant être facilités par la mise en réseau électronique et par l'identificateur de personne et de déléguer des décisions de très grande importance au niveau de l'ordonnance. Troisièmement, la protection de la personnalité prévue dans la Constitution implique certaines conditions pour l'introduction d'un identificateur de personne fédéral. Ces conditions ont été formulées par le Prof. G. Biaggini dans une expertise que nous avons mandatée (http://www.edsb.ch/d/themen/weitere/epid/gutachten-biaggini.pdf) [texte en allemand] comme suit (extrait traduit): «Compte tenu des exigences prévues dans la Constitution en ce qui concerne la protection de la personnalité, l'introduction d'un identificateur fédéral de personnes coordonné ne doit pas se faire sans mesures de protection complémentaires qui permettent d'éviter dans la mesure du possible les risques […]. Il est d'autant plus nécessaire d'agir que c'est l'Etat lui-même qui, par l'introduction d'un identificateur de personnes, crée les risques ou risques potentiels en cause. S'agissant d'un identificateur de personnes que la Confédération désire introduire, par «Etat», il faut comprendre en premier lieu la Confédération. Cela ne signifie pas que la responsabilité des cantons et des communes n'est pas pour autant engagée, car l'article 35 Cst. concerne tous les niveaux de l'Etat. En tant qu'instigateur, la Confédération doit cependant assumer une plus grande responsabilité, à laquelle elle ne peut pas simplement se soustraire en «déléguant» le problème aux cantons ou communes et à leurs organes (législateur, autres autorités).» C'est pourtant exactement ce que les projets présentés jusqu'ici font, en permettant aux cantons – par une délégation sans restrictions matérielles – d'utiliser l'identificateur de personne à des fins administratives. Relevons en outre qu'une telle démarche empêche dès le début de respecter le principe de finalité.

Compte tenu de ce qui précède, nous maintenons notre appréciation selon laquelle l'infrastructure qui doit être mise sur pied non seulement entraîne des coûts énormes, mais présente également des risques considérables pour la protection de la personnalité. Au vu de cette importance, il est nécessaire que les projets soient d'abord suffisamment concrétisés pour qu'une discussion politique et une décision deviennent possibles.

2 Protection des données – questions d'ordre général

2.1 Protection et sécurité des données

2.1.1 Eléments nécessaires d'un règlement de traitement

Nous recevons régulièrement des demandes de personnes désirant savoir ce que doit contenir un règlement de traitement. C'est pourquoi nous avons élaboré un modèle de table des matières mentionnant tous les points qui doivent figurer dans un tel règlement.

Le règlement de traitement est censé fournir la transparence nécessaire aussi bien dans le contexte du développement système que dans celui du traitement des données. La première version du règlement de traitement doit être disponible à la fin des phases de planification du projet et être mise à jour pendant l'exploitation du système. Un règlement de traitement doit, pendant la phase d'exploitation, documenter notamment les modifications apportées au système ainsi que les contrôles effectués. Il doit être rédigé de manière concise et bien compréhensible pour permettre également à des lecteurs non experts de comprendre et de juger le système. Il doit être fidèle au principe «autant que nécessaire et aussi peu que possible». Pour les informations plus détaillées, il doit renvoyer à d'autres documents. Il doit notamment permettre au maître du fichier d'obtenir une vue d'ensemble sur les systèmes ou applications qui ont accès aux fichiers respectifs. Le règlement doit clairement préciser le but du système. Il doit en outre documenter les flux d'information; ces derniers doivent montrer quelles informations de l'organe exploitant le système (maître du fichier) sont échangées avec d'autres organes, quand, comment et de quelle manière. Le règlement de traitement doit également documenter l'organisation. Ceci inclut d'une part l'organigramme de l'organe exploitant le système avec la mention des domaines dans lesquels on utilise le système et l'indication du nombre de collaborateurs. Il doit d'autre part également définir les responsabilités.

Les procédures constituent un autre domaine important de la documentation de l'organisation. Plus les données sont sensibles, plus les procédures doivent être détaillées. La documentation des tâches traditionnelles d'exécution des tâches débute lors de la collecte des données et se termine une fois que les données ont été archivées ou détruites.

En outre, il convient de définir les procédures de contrôle ainsi que les procédures pour l'exercice du droit d'accès. Le règlement de traitement doit également préciser la configuration des moyens informatiques ainsi que les mesures techniques et organisationnelles de sécurité des données. En ce qui concerne les mesures de sécurité, il y a lieu de définir comment ces dernières doivent être appliquées.

Un modèle détaillé de table des matières d'un règlement de traitement peut être téléchargé depuis notre site internet. (http://www.edsb.ch/f/doku/leitfaeden/tom/bearbeitungsreglement_f.pdf).

2.1.2 Expériences pratiques avec les traces électroniques

Après avoir décrit une façon de traiter correctement les traces électroniques sur la place de travail, nous avons poursuivi nos travaux dans ce domaine et procédé à l'analyse des différentes traces électroniques liées aux activités sur ordinateur des collaborateurs du PFPD. Cet état des lieux nous a permis de vérifier l'utilité des traces collectées et, dans le même temps, de sensibiliser les administrateurs aux aspects liés à la protection des données.

Les traces électroniques, et en particulier les fichiers journaux (logfiles), permettent de savoir «qui a fait quoi quand» et de découvrir, par exemple, la source d'une faute ou la provenance d'un virus, ou encore de récupérer l'ensemble des données à partir de copies de sauvegarde après une panne majeure. L'utilité des traces électroniques est indiscutable et la légitimité de les collecter est claire.

Le risque d'atteinte à la personnalité engendré par les traces électroniques n'est cependant pas toujours pris en compte, en particulier sur la place de travail. Or le traitement des traces électroniques qui contiennent des données personnelles est soumis la loi fédérale sur la protection des données. Nous avons décrit un traitement correct des traces électroniques dans le 11ème rapport d'activités, chiffre 2.1.3 (voir aussi http://www.edsb.ch/f/themen/sicherheit/technik/elektronische_spuren_f.pdf).

La suite du projet consistait à mettre en pratique les conseils prodigués et à établir d'abord un état des lieux. Nous avons ainsi entamé l'analyse des traces électroniques collectées dans le cadre de nos propres activités. L'organisation particulière de notre informatique implique l'intervention de deux instances tierces, chacune responsable d'une partie des traces électroniques collectées.

L'expérience nous a prouvé qu'il est tout à fait possible de respecter les conseils donnés. Avec un effort raisonnable et grâce à la coopération des instances tierces, il a été possible d'obtenir une liste complète des traces électroniques collectées.

Les informations obtenues jusqu'à présent nous ont permis de découvrir que certaines traces ne sont en réalité pas utiles (c'est le cas de la liste des fichiers compressés et décompressés) et que d'autres évènements exploitables ne sont au contraire pas tracés, comme par exemple les changements de mot de passe des utilisateurs. Nous allons continuer nos investigations, puis nous tenterons de corriger les imperfections constatées.

2.1.3 Le «pervasive computing» et son impact sur la sphère privée

On peut prévoir que d'ici la prochaine décennie, la société sera envahie par le «pervasive computing». Des problèmes d'atteinte à la personnalité sont prévisibles. Une collaboration avec les spécialistes du domaine est recommandée pour trouver une solution équilibrée, réaliste, et donc optimale.

Le «pervasive computing» (informatique ubiquitaire) ouvre la porte à une multitude d'applications très utiles. Avec des technologies comme RFID (Radio Frequency Identification), GPS (Global Positioning System) ou UMTS (Universal Mobile Telecommunications Systems), on pourra par exemple développer des applications pour réduire les risques de vol de voitures ou pour gérer plus efficacement un magasin. Malheureusement, le pervasive computing comporte aussi des risques d'atteinte à la personnalité. Par exemple, une technologie comme le GPS permet également de tracer les déplacements d'une personne.

La meilleure façon de prévenir les problèmes de protection des données est de les limiter ou de les éviter, par exemple en réduisant la quantité de données personnelles traitées. Pour atteindre cet objectif, il faut anticiper les risques encourus et agir d'une façon aussi proactive que possible. A cet effet, nous avons lancé un projet d'évaluation des risques et perspectives liés à ce phénomène.

Pendant la première phase du projet, nous avons amélioré notre savoir-faire, en particulier en classant les différentes applications existantes en fonction des différentes technologies utilisées. Pour chaque application identifiée, nous avons aussi déterminé les risques potentiels liés à la protection des données et nous les avons analysés et classés selon le degré d'atteinte à la personnalité. Notre intention est d'avoir une vue d'ensemble. La deuxième phase du projet visera à consolider les résultats en collaboration avec des spécialistes du domaine. Seule une approche multidisciplinaire pourra amener à une solution équilibrée, rationnelle et donc optimale.

2.1.4 Amélioration de la protection des données par le chiffrement des messages SMS

La surveillance, parfois abusive, des canaux de télécommunication représente une importante atteinte à la personnalité. La quantité de messages SMS envoyés a fortement augmenté au cours de ces dernières années, sans que des moyens de protection n'aient été mis à disposition des utilisateurs. Une collaboration avec un chercheur finlandais nous a permis de tester la version expérimentale d'une application de chiffrement de messages SMS, ce qui nous a convaincu que cette technique pouvait être utilisée par le grand public.

Au cours des cinq dernières années, la quantité de données personnelles échangées par SMS a augmenté de façon exponentielle. Par conséquent, le risque d'une atteinte à la personnalité et l'intérêt pour accéder à ces données ont aussi augmenté.

Nous avons donc cherché des solutions permettant de résoudre ce problème. Nous sommes partis à la recherche d'une application de chiffrement; l'application de chiffrement permet en effet d'éliminer le problème à la racine, puisqu'elle transforme les données dans une forme incompréhensible pour d'éventuels attaquants. Après quelques investigations, nous avons choisi une application développée par des chercheurs finlandais. L'application en question, appelée «SafeSMS», est écrite en langage Java et est compatible avec les téléphones cellulaires modernes (MIDP 2.0). La version testée n'est pas encore prête pour une distribution à large échelle, car il y a quelques fautes mineures et la convivialité pourrait encore être améliorée. L'aspect central de nos tests est de démontrer qu'un chiffrement robuste des SMS est possible avec un temps d'exécution raisonnable (quelques secondes). L'algorithme de chiffrement utilisé est Blowfish, qui donne une sécurité suffisante, pour autant que la clé choisie soit suffisamment complexe. Une version AES (Advanced Encryption Standard) est aussi envisagée par les développeurs. S'agissant d'un chiffrement symétrique, les deux partenaires de la communication doivent s'accorder sur un mot de passe secret commun. «SafeSMS» permet d'avoir un répertoire téléphonique des partenaires de communication, contenant leurs mots de passe respectifs. Ce répertoire est protégé par un mot de passe principal connu seulement de son détenteur. Hormis la rapidité, l'avantage du chiffrement symétrique est qu'il ne nécessite pas d'infrastructure à clés publiques (PKI), laquelle, à cause de sa complexité, n'est pas envisageable à aussi court terme.

Les développements dans de telles applications de chiffrement peuvent représenter une excellente voie pour protéger des données personnelles. Nous allons donc continuer à surveiller les progrès dans ce domaine.

2.2 Autre thèmes

2.2.1 Problèmes de protection des données en rapport avec la mise en œuvre d'Armée XXI

Dans le cadre de la mise en œuvre d'Armée XXI, nous avons attiré à plusieurs reprises l'attention du DDPS sur le fait que dans de nombreux domaines, il manquait les bases légales suffisantes pour le traitement de données personnelles sensibles ou de profils de la personnalité. Le DDPS envisage aussi à l'avenir de traiter des données personnelles sensibles sans bases légales suffisantes.

Dans notre dernier rapport d'activités, nous avons examiné à la lumière des principes de la protection des données l'utilisation du questionnaire médico-psychologique accompagnant le recrutement des conscrits (voir notre 11ème rapport d'activités 2003/2004, chiffre 2.2.1). Au cours de l'année écoulée, nous nous sommes prononcés sur plusieurs projets d'ordonnance du DDPS (entre autres la révision partielle de l'ordonnance sur les contrôles militaires ou sur la révision totale de l'ordonnance concernant l'appréciation médicale de l'aptitude au service et de l'aptitude à faire service) qui ont été soumis à l'approbation du Conseil fédéral dans le cadre de la mise en œuvre d'Armée XXI.

Du point de vue de la protection des données, les problèmes qui se sont présentés étaient dans chaque cas les mêmes:

D'une part, les bases légales suffisantes requises par la loi sur la protection des données pour le traitement de données personnelles sensibles ou de profils de la personnalité ne figurent pas dans la loi sur l'armée (violation du principe de légalité). D'autre part, les ordonnances élaborées par le DDPS n'ont pas été concrétisées de façon suffisante: Les dispositions relatives au traitement des données sont incomplètes et trop vagues (violation des principes de légalité et de transparence). Le DDPS a notamment décidé dernièrement de ne pas introduire dans les annexes aux ordonnances un catalogue détaillé des données ainsi que les autorisations d'accès et les modalités de traitement.

Après plusieurs interventions de notre part, le Secrétariat général du DDPS nous a fait savoir que le Département entendait maintenir la ligne suivie jusqu'ici et qu'il ne créerait pas, même dans un proche avenir, les bases légales formelles suffisantes pour le traitement de données personnelles sensibles. Le DDPS a ajouté qu'il avait l'intention

«de créer en premier lieu *en cas de nécessité* les bases légales matérielles au niveau de l'ordonnance et *le cas échéant* de compléter la loi sur l'armée dans le cadre de la prochaine révision.»

Le fait que le DDPS approuve l'inobservation du principe de légalité et accepte en connaissance de cause la violation de la personnalité des membres de l'armée est particulièrement alarmant. Nous avons de ce fait requis à plusieurs reprises que l'on n'attende pas jusqu'en 2009 pour créer les bases suffisantes dans la loi sur l'armée, mais que l'on entreprenne immédiatement une révision partielle anticipée de cette loi. Le DDPS rejette également cette proposition. Néanmoins, le Secrétariat général nous a assurés qu'à l'avenir, les annexes des ordonnances comporteraient à nouveau un catalogue complet des données avec les modalités de traitement et les autorisations d'accès.

2.2.2 Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé

L'utilisation de la biométrie est de plus en plus répandue et s'étend désormais à toute la société civile, dans des procédures automatisées d'authentification et d'identification allant de l'accès à des cantines scolaires au contrôle d'accès à des installations ou à des systèmes informatiques, en passant par le paiement de titre de transport, au contrôle du temps de travail, des tests de présence. Le recours à la biométrie présente des risques pour les libertés et les droits fondamentaux et est ainsi devenu un enjeu de taille pour la protection des données. Le PFPD propose quelques principes à respecter en matière de protection des données.

Dans un rapport présenté lors de la 26ème Conférence internationale des commissaires à la protection des données (voir chiffre 9.4.1 et http://www.edsb.ch/f/doku/fachpresse/index.htm), le PFPD a proposé quelques principes pour garantir la protection des données lors de l'utilisation de données biométriques. Du point de vue de la protection des données, l'utilisation de la biométrie peut présenter des risques importants, liés notamment aux possibilités de suivi des individus et d'interconnexion des informations et des fichiers. Le recours à la biométrie peut également se révéler bénéfique, notamment pour sécuriser l'accès à des données. La biométrie pourrait ainsi devenir un instrument au service de la protection de la vie privée. Il faut toutefois rester conscient qu'elle ne peut pas être la solution à tous les problèmes de contrôle et de gestion. Les procédures biométriques présentent des défauts et des faiblesses tant sous l'angle de la fiabilité des résultats (rejet ou acceptation erronés) que de la

sécurité des données. Le recours à la biométrie peut aussi être une source de discrimination et porter atteinte à la dignité humaine (voir chiffre 9.4.1). Ainsi, il conviendrait de prendre en considération les principes suivants lors du recours à des données biométriques dans le secteur privé

- On ne recourra à la biométrie que s'il n'y a pas d'autres moyens moins intrusifs d'atteindre l'objectif visé.
- De même, on pourra recourir à la biométrie si celle-ci a pour but la protection et la sécurité des données.
- La finalité du traitement doit être strictement respectée.
- Les personnes concernées doivent être clairement informées et associées au processus de traitement.
- La collecte des données biométriques doit se faire directement auprès de la personne concernée ou au moins portée à sa connaissance.
- Pour éviter des discriminations, il est nécessaire de prévoir des alternatives pour les personnes qui ne sont pas en mesure d'utiliser un système biométrique.
- L'identification de données biométriques doit se faire uniquement en comparant un échantillon prélevé auprès de la personne concernée.
- Les données biométriques originales doivent être détruites une fois la procédure d'enrôlement effectuée.
- Il faut privilégier des technologies basées sur le stockage de gabarit plutôt que de données brutes et sur l'utilisation de données biométriques n'impliquant pas le stockage de gabarits dans une base de données gérée par un responsable de traitement autre que la personne concernée. Cette procédure ne soulève en principe pas de problèmes particuliers du point de vue de la protection des données, dès lors que le gabarit est conservé sur un support dont la personne concernée a l'usage exclusif (carte à puce, téléphone mobile, ordinateur portable, etc.).
- Si une base de données est constituée et gérée par un responsable de traitement autre que la personne concernée, l'élément biométrique retenu peut avoir des conséquences sur les libertés et droits fondamentaux. Tel est en particulier le cas lorsque l'élément biométrique laisse des traces, comme l'empreinte digitale. Le recours à un tel élément doit répondre à un intérêt prépondérant qualifié de sécurité.
- En l'absence d'un tel intérêt, il convient de recourir à un élément biométrique qui limite le risque d'abus, tel que celui ne laissant pas de trace, comme le contour de la main.

- Lors du recours à des éléments qui laissent des traces et qui sont stockés dans une banque de données, il convient de prendre les mesures nécessaires pour éviter un détournement de finalité, notamment en chiffrant l'élément contenu dans la base de données à l'aide du gabarit, de sorte que le déchiffrement ne puisse se faire qu'en présence de la personne à laquelle l'information biométrique se rapporte. Le gabarit doit être propre à l'application concernée pour éviter les possibilités de relier des données ou d'avoir accès à des applications différentes.
- Il faut prendre les mesures nécessaires pour éviter d'utiliser l'information biométrique comme un identifiant unique universel.
- Il faut éviter que l'on puisse déduire, à partir des données biométriques, d'autres données sur la personne, notamment des données relatives à son état de santé.
- Dans un système d'authentification (vérification), il convient d'éviter de collecter et de traiter d'autres données personnelles que celles nécessaires à l'authentification et, par conséquent, de privilégier des solutions ne nécessitant pas de révéler l'identité de la personne (authentification anonyme), à moins que l'identification ne soit indispensable à la finalité du traitement (principe de l'économicité du traitement).
- Dans un système d'authentification, les données biométriques ne doivent pas être utilisées à d'autres fins que la vérification, sauf si la loi le prévoit expressément (notamment dans le cadre d'une poursuite pénale).
- Pour améliorer la sécurité des données et diminuer les risques d'accès non autorisé, notamment s'appropriant les données de tiers, il convient de renforcer le système biométrique avec d'autres moyens d'identification ou d'authentification (par ex. code d'accès). Il convient également d'avoir des lecteurs biométriques sécurisés permettant aux personnes légitimées de présenter directement leurs données ou de recourir à des systèmes dans lesquels les données biométriques sont intégrées à un dispositif sécurisé, comme une carte à puce.
- Les données biométriques doivent être chiffrées dès leur enrôlement. La communication électronique de ces données, notamment au travers d'un réseau, doit également être chiffrée.
- La fiabilité des données biométriques enregistrées (gabarit) doit être périodiquement vérifiée (ré-enrôlement périodique). L'échantillon biométrique présenté par la personne peut en effet varier avec le temps.
- Les droits des personnes concernées doivent être garantis. En particulier, les personnes concernées doivent avoir la possibilité de contrôler l'usage qui est fait de leurs données biométriques et d'en obtenir la destruction le cas échéant.

- Les systèmes d'informations biométriques devraient faire l'objet d'une procédure de certification et d'audit en matière de protection des données. Ces systèmes devraient également être évalués sous l'angle des risques avant leur mise en fonction. Un concept de protection devrait être élaboré, définissant notamment les processus de traitement.

Pour un exemple d'application de la biométrie dans le secteur privé, voir également chiffre 7.2 du présent rapport d'activités.

2.2.3 Projet de loi sur l'information géographique

Dans le cadre de la mise en œuvre d'une loi sur l'information géographique et de l'élaboration des ordonnances d'application, plusieurs éléments importants du point de vue de la protection des données comme par exemple la transparence des traitements, la finalité, la réglementation claire de la communication de données personnelles ou la garantie des droits des personnes concernées doivent être pris en compte.

Lors de la consultation relative au projet de loi sur l'information géographique, nous avons rappelé à l'Office fédéral de topographie que dans le cadre de la mise en œuvre de cette loi et de l'élaboration des ordonnances d'application, plusieurs éléments importants du point de vue de la protection des données doivent être pris en compte. La réalisation et l'exploitation d'un système d'informations géographiques (SIG) qui contient des données personnelles ou qui peut aisément être mis en relation avec de telles données doivent intervenir dans le respect de la LPD.

Il est important de veiller à la *transparence des traitements*. A cet effet, il faut que les personnes concernées puissent être informées sur les finalités du système, les catégories de données traitées, les utilisateurs du système et les destinataires des informations et qu'elles puissent faire valoir leurs droits, notamment par le biais du droit d'accès.

La *finalité* du SIG doit être *déterminée, spécifique et légitime* et les données doivent être traitées conformément à cette finalité. Par exemple, un SIG conçu pour des applications ne se référant pas à des personnes déterminées ou accessible à chacun devrait intégrer des mécanismes limitant ou interdisant la mise en relation avec des données personnelles, notamment pour garantir l'anonymat des personnes lors de la publication ou de la diffusion.

Le *catalogue des données traitées* doit être *défini*. Seules les données nécessaires à la finalité du SIG doivent être collectées et traitées. On évitera, dans la mesure du possible, d'intégrer des données sur des personnes identifiées ou des données permettant d'identifier les personnes.

La *qualité des données* doit être *garantie* (exactitude, mise à jour, conservation limitée dans le temps).

La *communication de données personnelles*, en particulier leur diffusion ou publication par procédure d'appel, doit être *clairement réglée*.

Le cadre juridique doit également être accompagné de *mesures techniques et organisationnelles* pour éviter des accès non autorisés ou limiter les risques d'identification non justifiée des personnes.

Les *droits des personnes* doivent être *garantis*. En particulier, le droit à l'information préalable, le droit d'accès aux données qui les concernent et notamment le droit de s'opposer à la collecte systématique et au traitement à des fins commerciales des données sous forme d'images de leur environnement d'habitation.

Les principes de base de la protection des données doivent être intégrés dans le développement des SIG. Il faut utiliser les technologies mettre en œuvre les exigences légales. A cette fin, les responsables de traitement doivent acquérir les connaissances nécessaires pour intégrer dès le début les aspects de la protection des données dans la réalisation de ces projets. Cela nécessite en particulier la mise en place d'un concept de protection des données à réaliser lors du développement d'un SIG.

3 Justice/Police/Sécurité

3.1 Affaires de police

3.1.1 Information ultérieure des personnes concernées dans le domaine de la police

Nous avons procédé à un examen des faits dans le domaine de la police concernant l'information ultérieure – prévue par la loi – des personnes dont des données sont traitées. Nous avons constaté qu'il n'y avait jamais eu d'information ultérieure jusqu'au moment de notre examen. Dans un premier cas, l'Office fédéral de la police doit encore élaborer un concept pour l'application de la disposition légale. Dans un deuxième cas, quelques personnes ont entre-temps été informées.

Dans le cadre de notre compétence comme organe de surveillance des organes fédéraux, nous avons décidé de procéder à un examen des faits à l'Office fédéral de la police (OFP) concernant l'information ultérieure dans le domaine de la police. Il y a lieu de distinguer 2 cas:

Le premier cas concerne le traitement de données personnelles dans les banques de données JANUS (crime organisé, trafic illicite de stupéfiants, faux-monnayage, traite des êtres humains, blanchiment d'argent, etc.) et GEWA (banque de données du Bureau de communication en matière de blanchiment d'argent). Dans ce premier cas, des données personnelles peuvent être recueillies par l'OFP à l'insu des personnes concernées, pour autant que la finalité de la poursuite pénale exige le maintien du secret. Dans un tel cas, il est néanmoins nécessaire d'informer la personne concernée ultérieurement, pour autant que des intérêts importants liés à la poursuite pénale ne s'y opposent pas et que cela n'entraîne pas un volume de travail excessif. Cette première forme de l'information ultérieure est réglée à l'art. 14 al. 1 LOC (Loi fédérale sur les Offices centraux de police criminelle de la Confédération).

Le deuxième cas concerne les banques de données JANUS et GEWA (déjà mentionnées ci-dessus) ainsi que la banque de données ISIS (protection préventive de l'Etat). Il s'agit de personnes qui ont déposé une demande de renseignement indirecte et qui sont, ou ont été, enregistrées dans un ou plusieurs des systèmes d'information précités. Selon la loi, ces personnes doivent être renseignées dès lors que les intérêts liés au maintien de la sécurité intérieure ou les intérêts liés à la procédure pénale ne requièrent plus le maintien du secret, mais au plus tard lors de l'expiration de l'obligation de conserver les données, et pour autant que cela n'entraîne pas un volume de travail

excessif. Cette information se fait selon la loi sur la protection des données. Cette manière d'informer a posteriori la personne concernée est réglée aux articles 18 al. 6 LMSI (pour ISIS) et 14 al. 4 LOC (pour JANUS et GEWA).

Nous avons voulu savoir comment l'OFP applique ces dispositions légales concernant l'information ultérieure. Nous avons annoncé à l'OFP que nous allions procéder à un examen des faits et en avons profité pour lui poser quelques questions. Nous nous sommes par la suite rendus sur place.

Nous avons constaté que l'information ultérieure selon l'art. 14 al. 1 LOC (premier cas) n'avait jamais été appliquée, car – selon l'OFP – elle aurait exigé une charge de travail excessive. En ce qui concerne l'information ultérieure selon les art. 14 al. 4 LOC et l'art. 18 al. 6 LMSI (deuxième cas), personne n'en a encore bénéficié. En ce qui concerne ISIS, l'OFP a fait valoir qu'il existait encore des intérêts au maintien du secret; s'agissant de JANUS, l'OFP a affirmé que cette disposition ne pouvait pas encore être appliquée du point de vue technique.

Là-dessus, nous avons adressé des recommandations à l'OFP. En ce qui concerne l'art. 14 al. 1 LOC, nous avons demandé à l'OFP d'élaborer une procédure ou un concept permettant de mettre en pratique l'information ultérieure telle que prévue dans la loi. Nous avons également demandé un réexamen de tous les cas survenus après l'introduction de la disposition légale. Quant à l'information ultérieure réglée aux art. 14 al. 4 LOC et 18 al. 6 LMSI, nous avons prié l'OFP d'examiner une nouvelle fois les banques de données pour identifier tous les cas dans lesquels une personne effectivement enregistrée avait déposé une demande de renseignement indirecte.

S'agissant de l'application de l'art. 14 al. 1 LOC, l'OFP va élaborer un concept qu'il va nous soumettre. En ce qui concerne l'information ultérieure des personnes qui ont déposé une demande de renseignement indirecte, l'OFP a accepté nos recommandations. En ce qui concerne les art. 14 al. 4 LOC et 18 al. 6 LMSI, l'application technique de toutes nos exigences nécessitera, selon l'OFP, encore un peu de temps. Ceci devrait néanmoins encore être le cas dans le courant de l'année 2005.

3.1.2 Message relatif à l'accord Europol

Nous avons eu l'occasion de prendre position sur l'accord passé entre la Suisse et Europol. Nous avons à cette occasion critiqué qu'il ne ressortait pas du message quelles sont les banques de données suisses livrant des données à Europol. Le message devrait en outre indiquer pour chaque banque de données suisse concernée s'il existe une base légale dans le droit suisse ou si celle-ci doit d'abord être créée. Il est incontesté que le PFPD est considéré dans le cadre d'Europol comme instance de contrôle nationale indépendante.

Suite aux négociations en cours sur les accords bilatéraux II, l'Union européenne a décidé de bloquer l'accord passé entre la Confédération suisse et l'Office européen de police (accord Europol). Après une pause qui a duré près de deux ans, l'accord entre la Suisse et Europol a été signé le 24 septembre 2004. Nous avons eu l'occasion, dans le cadre de la consultation des offices, de prendre position sur le message concernant cet accord.

Tout d'abord, nous avons constaté avec satisfaction que le message attire explicitement l'attention sur le fait qu'il est nécessaire de créer dans le droit suisse des bases légales au sens formel permettant expressément de communiquer des données personnelles. Ceci découle du texte de l'accord qui renvoie au droit national en ce qui concerne la communication des informations. Nous avions déjà attiré l'attention sur ce point lors de l'une de nos précédentes interventions.

Nous sommes toutefois quelque peu inquiets en ce qui concerne les bases légales qui sont prévues. A ce sujet, il a été proposé de créer un seul article dans une loi au sens formel. Nous avons voulu examiner si cette disposition unique permettrait de régler toutes les communications de données personnelles à Europol. Afin de l'évaluer, nous avions besoin de savoir quelles sont les banques de données suisses à partir desquelles des données sont communiquées à Europol. Toutefois cette information ne ressort justement pas du texte du message. Ce dernier mentionnait uniquement que les données personnelles pouvaient provenir de diverses sources. Dans notre prise de position, nous avons attiré l'attention sur le fait que le message même devait contenir la liste de toutes les banques de données à partir desquelles la Suisse transférerait des données vers Europol. Il faudrait ensuite déterminer, pour chacune des banques de données concernées, si une loi au sens formel – et en l'occurrence laquelle – permet la communication de données à Europol. Au cas où il n'existerait pas de base légale au sens formel pour l'une des banques de données, celle-ci devrait d'abord être créée. La même chose s'applique à toute extension de l'accord à d'autres catégories de délits.

En outre, nous avons demandé que notre rôle d'autorité nationale de contrôle soit expressément mentionné.

Nous avons demandé à l'office compétent de prendre en compte nos remarques, respectivement de mentionner la divergence dans la proposition au Conseil fédéral.

3.1.3 Adaptation de la procédure relative au droit d'accès indirect conformément aux articles 14 LOC et 18 LMSI

Suite à une décision de la Commission fédérale de la protection des données (CFPD), nous avons dû adapter notre procédure en matière de droit d'accès indirect dans les systèmes d'informations ISIS, JANUS et GEWA de l'Office fédéral de la police. La principale nouveauté est l'établissement d'un rapport de contrôle relatif à l'examen de la demande de droit d'accès indirect. Ce rapport ne contient pas d'information de nature policière.

Dans une décision, la Commission fédérale de la protection des données (CFPD) a recommandé au Préposé fédéral à la protection des données (PFPD) d'adapter sa procédure en matière de droit d'accès indirect. Certaines recommandations ont pu être directement appliquées, tandis que d'autres nécessitent encore des éclaircissements.

La CFPD a jugé que la note établie lors de l'examen des demandes de droit d'accès dans les systèmes d'informations ISIS, JANUS et GEWA de l'Office fédéral de la police (OFP) devait être élaborée sous forme d'un rapport plus détaillé. Cette recommandation a été immédiatement suivie et le PFPD établit désormais un rapport contenant la liste des inscriptions et documents présentés par l'OFP et examinés par le PFPD. Pour chaque inscription ou document, plusieurs éléments sont notés dans le rapport (par exemple: la référence, la date, la fiabilité, la nature de l'inscription et du document, l'expéditeur et le destinataire). Il est important de préciser que le rapport ne contient aucune information de nature policière. Le rapport indique également les inscriptions et documents problématiques quant à la légalité, à la proportionnalité ou à l'exactitude des données. Les références des recommandations émises par le PFPD sont le cas échéant indiquées dans le rapport.

Certains points de la décision de la CFPD doivent encore être clarifiés en collaboration avec la CFPD et l'OFP.

3.2 Autres thèmes

3.2.1 Révision de l'ordonnance sur le Bureau de communication en matière de blanchiment d'argent

L'avant-projet de l'ordonnance révisée sur le Bureau de communication en matière de blanchiment d'argent contient toujours des dispositions qui devraient en fait figurer dans une loi au sens formel. C'est pourquoi il conviendrait de réviser d'abord les bases légales au sens formel. Par ailleurs, des problèmes pratiques sont apparus en ce qui concerne le droit d'accès indirect prévu dans l'ordonnance.

Dans le cadre de la consultation des offices, nous avons pu prendre position sur l'avant-projet de l'ordonnance révisée sur le Bureau de communication en matière de blanchiment d'argent (OBCBA). On mentionnera tout d'abord que la loi sur la protection des données exige pour le traitement de données sensibles par les organes fédéraux une base légale au sens formel. A ce propos, nous avons constaté que l'avant-projet de l'OBCBA contenait de nombreuses dispositions qui devraient – au moins dans leurs grandes lignes – faire l'objet d'une base légale au sens formel. C'est pourquoi nous avons retenu qu'il conviendrait, avant de réviser l'OBCBA, de créer tout d'abord les bases légales au sens formel qui sont nécessaires. On rappellera que, dans le cadre de l'élaboration et de la mise en vigueur de la Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier (LBA), nous avions déjà fait remarquer que les bases légales au sens formel prévues pour la LBA ne suffiraient pas à autoriser les traitements de données du Bureau de communication en matière de blanchiment d'argent. La LBA est tout de même entrée en vigueur. Par contre, la durée de validité de l'OBCBA a été limitée et il a été prévu de rédiger un rapport (voir notre 5ème rapport d'activités 1997/98, chiffre I 1.3). Il était donc déjà clair au moment de l'élaboration de l'OBCBA que celle-ci contenait un grand nombre de dispositions qui devraient figurer dans une loi au sens formel. Compte tenu de ce qui précède, nous attachons une grande importance au fait que l'OBCBA révisée ne reste en vigueur que pour une durée limitée, jusqu'à ce que les bases légales au sens formel soient créées.

L'avant-projet prévoit toujours pour le système d'information du Bureau de communication le droit d'accès indirect. Mis à part le fait qu'ici aussi une loi au sens formel serait nécessaire, nous relevons que ce droit d'accès indirect ne correspond pas au droit d'accès tel qu'il est prévu par la loi sur la protection des données. En effet, les personnes concernées ont pour seule garantie que leur demande est traitée par un

organe externe à l'Office fédéral de la police. Dans ces conditions, il ne nous est pratiquement pas possible de vérifier la véracité des inscriptions existantes. Les personnes concernées ne peuvent ainsi guère exercer leur droit de rectification. De plus, en ce qui concerne le droit d'accès indirect, nous sommes toujours confrontés à des problèmes d'ordre procédural et juridique. C'est pourquoi nous avons proposé de soumettre le système d'information aux dispositions de la loi fédérale sur la protection des données concernant le droit d'accès *direct*, avec les possibilités de restrictions prévues par la même loi.

Nos requêtes concernant le défaut de bases légales au sens formel et le droit d'accès indirect n'ont pas été prises en compte par l'office fédéral compétent. Notre divergence a été mentionnée dans la proposition adressée au Conseil fédéral.

Il reste à espérer que les bases légales au sens formel qui font défaut seront le plus rapidement possible introduites.

3.2.2 Révision de la législation sur les étrangers et de la législation sur l'asile

Pour être conforme aux principes généraux de protection des données, la communication à des autorités étrangères d'informations relatives à des procédures pénales doit avoir une finalité légitime. Le but d'éviter des blocages dans le cadre de négociations d'accords de réadmission ou de transit ne constitue pas une telle finalité. De plus, le relevé des empreintes digitales et de la photographie des personnes entrant de manière illégale en Suisse doit reposer sur une loi au sens formel.

Lors de l'examen par les Chambres fédérales des projets de révision totale de la loi sur les étrangers et de révision partielle de la loi sur l'asile, l'Office fédéral des réfugiés (ODR; actuellement Office fédéral des migrations) a proposé d'ajouter dans ces deux lois des dispositions permettant la communication d'informations relatives à des procédures pénales en Suisse aux autorités des Etats d'origine, de résidence, de transit ou tiers ainsi qu'à des organisations internationales. Selon l'ODR, une telle communication a pour but d'éviter des blocages dans le cadre de négociations d'accords de réadmission et de transit. La finalité invoquée, à savoir la communication de données sensibles afin de faciliter les négociations avec un Etat étranger, ne peut être considérée comme légitime; la communication envisagée n'est dès lors pas conforme aux principes généraux de protection des données. La communication d'informations relatives à des procédures pénales doit avoir lieu conformément à la législation sur l'entraide internationale en matière pénale qui prévoit des règles de protection de la

personnalité. La communication systématique – en dehors d'une procédure pénale à l'étranger – contournerait ces règles de protection et exposerait ainsi les personnes à de sérieux risques d'atteinte à leur personnalité. De plus, une telle communication systématique, y compris à des destinataires qui ne devraient pas obtenir de telles informations (Etats tiers ou de transit et organisations internationales), serait totalement disproportionnée.

Afin de permettre de relever les empreintes digitales et la photographie des personnes entrant de manière illégale en Suisse, l'Office fédéral de l'immigration, de l'intégration et de l'émigration (IMES; actuellement Office fédéral des migrations) a proposé de modifier deux ordonnances du Conseil fédéral. Les mesures envisagées constituent une atteinte à la personnalité des personnes concernées ainsi qu'un traitement de données sensibles au sens de la LPD. Un tel traitement par un organe fédéral n'est possible que si une base légale au sens formel le prévoit expressément. L'IMES a invoqué une disposition de la loi fédérale sur le séjour et l'établissement des étrangers qui ne peut servir de base légale suffisante. En effet, cette disposition précise clairement qu'on peut recourir aux empreintes digitales et à l'image faciale pour établir l'identité d'un étranger. Elle ne couvre ainsi pas le cas de l'étranger identifié qui tente d'entrer illégalement en Suisse. Les dispositions de deux ordonnances ne pouvant servir de base légale suffisante au regard de la LPD, nous avons soutenu dans notre prise de position qu'il était nécessaire d'élaborer une base légale au sens formel prévoyant expressément le relevé des empreintes digitales et de l'image faciale des personnes entrant de manière illégale en Suisse. Le Conseil fédéral n'a pas tenu compte de nos remarques et les deux modifications sont entrées en vigueur le 1er juin 2004.

3.2.3 Publication dans la presse de données personnelles relatives à des enquêtes de police ou à des jugements

La publication de données relatives à des enquêtes de police ou à des jugements doit respecter la règle de l'anonymat, sauf si la personne concernée y consent, si une loi le prévoit ou si un intérêt privé ou public prépondérant le justifie, et dans la mesure où la publication ne contrevient pas à une autre norme juridique. Il peut notamment exister un intérêt public à la publication de données personnelles dans la presse lorsque le prévenu ou le condamné est, ou a été, une personnalité politique, un magistrat de l'ordre judiciaire, une personne exerçant, ou ayant exercé, d'importantes fonctions dans l'administration publique, une personne occupant une position avec d'importantes responsabilités économiques ou sociales, ou disposant de qualités sportives, sociales ou artistiques sortant de l'ordinaire.

La publication d'informations par la presse constitue un traitement de données personnelles au sens de la LPD, dans la mesure où ces informations se rapportent à des personnes identifiées ou identifiables. Selon la LPD, personne n'est en droit, sans motif justificatif, de communiquer des données personnelles (c'est-à-dire non anonymes) à des tiers. Les motifs justificatifs sont les suivants: le consentement de la personne concernée, l'intérêt privé ou public prépondérant et la loi. De façon générale, la LPD reconnaît l'existence d'un intérêt prépondérant pour collecter des données personnelles en vue d'une publication (travail de recherche journalistique précédant la publication). Ce motif justificatif ne peut cependant pas être invoqué pour la publication de données personnelles dans la presse.

Toutefois, la LPD n'exclut pas l'existence d'autres intérêts prépondérants. On peut notamment considérer comme tel le devoir des médias d'informer le public sur des questions d'intérêt général, notamment sur des affaires dont connaissent les tribunaux ou les enquêteurs de police, dans la mesure où le besoin d'informer le public n'entre pas en conflit avec le secret de l'enquête.

Même si la publication de données personnelles repose sur un intérêt public prépondérant, elle doit en outre respecter les principes généraux de la LPD, notamment les principes de la licéité et de la proportionnalité.

Une question qui se pose est celle de savoir si la presse est autorisée, dans le cadre d'une enquête de police ou d'un jugement, à divulguer de façon transparente les informations dont elle dispose. Dans le contexte particulier de l'enquête de police, il est nécessaire de tenir compte de l'absence de condamnation du suspect et de la présomption d'innocence. En effet, le public ne fait souvent pas la différence entre un suspect et un coupable. Donner le nom et la photo d'un suspect, c'est en faire, aux yeux d'un nombre considérable de personnes, un coupable. Alors qu'il bénéficie encore de la présomption d'innocence aux yeux de la loi, le suspect sera jugé par ses concitoyens, en contradiction avec les plus élémentaires principes de l'équité. La situation sera particulièrement choquante en cas d'acquittement.

L'anonymat ne se justifie pas seulement en raison de la présomption d'innocence, mais il permet aussi une meilleure réinsertion sociale de la personne soupçonnée ou condamnée. La règle de l'anonymat est le corollaire du principe de la proportionnalité et de la présomption d'innocence. En principe, les médias ne peuvent donc désigner ni un suspect, ni une personne condamnée, par son nom ou par tout autre élément permettant son identification. Représentent des éléments d'identification de la personne sa photo, sa caricature, son adresse, ses plaques minéralogiques, la désignation de sa fonction ou de sa profession, autant d'éléments qui ne laissent aucun doute sur l'identité de la personne concernée. Des initiales ne sont souvent pas suffisantes pour cacher l'identité du prévenu ou de l'auteur de l'infraction. Tel est le cas lorsque celles-ci sont particulièrement originales ou que la personne concernée provient d'une petite localité qui a été indiquée en toutes lettres, ou lorsque les initiales sont accompagnées de renseignements ponctuels qui, ajoutés les uns aux autres, ont pour effet de désigner la personne sans aucun doute possible (nationalité, situation familiale, etc.). L'usage courant qui consiste à indiquer le prénom et la première lettre du nom de famille est encore plus risqué à cet égard.

Le consentement de la personne concernée, *l'intérêt privé ou public prépondérant* et *la loi* sont des exceptions à la règle de l'anonymat, respectivement à l'interdiction aux médias de désigner l'auteur d'une infraction ou un suspect par son nom ou par tout autre élément permettant son identification.

Ainsi, si le prévenu attire volontairement l'attention sur lui, notamment en donnant des interviews, on peut considérer qu'il *a consenti* à la divulgation de son identité. Dans ce cas, la publication de l'identité du prévenu serait en principe licite. Cependant, la publication du nom peut heurter les normes procédurales assurant le secret de l'enquête. Il convient par conséquent de tenir compte des intérêts du prévenu, des magistrats et des autres personnes concernées par l'enquête, notamment en évitant de révéler les noms des personnes concernées.

Il peut exister un *intérêt public prépondérant* à la publication de données personnelles dans la presse lorsque le prévenu ou le condamné est, ou a été, une personnalité politique ou un magistrat de l'ordre judiciaire, une personne exerçant, ou ayant exercé, d'importantes fonctions dans l'administration publique, une personne occupant une position avec d'importantes responsabilités économiques ou sociales, ou encore disposant de qualités sportives, artistiques ou scientifiques sortant de l'ordinaire. Celui qui, régulièrement, attire sur lui la curiosité des médias en raison de sa position doit admettre que cette curiosité demeure même dans des situations moins favorables pour lui. L'infraction, en principe, doit être en relation avec la position occupée par la personne et qui lui vaut sa notoriété

La gravité de l'infraction, l'originalité des faits en cause, le degré de perversité de l'auteur ne peuvent à eux seuls justifier la publication du nom ou d'autres éléments permettant son identification, et cela ni avant, ni après la condamnation. Pour justifier la publication, il faut établir que la personne concernée présente un risque sérieux et concret touchant un grand nombre de personnes et que la publication de son nom au moment du jugement est de nature à réduire ce risque de manière importante.

La loi autorise les autorités judiciaires à publier des avis de recherche contenant le nom, la photo ou le portrait-robot de la personne recherchée. Le Tribunal fédéral admet la publication du nom d'un prévenu qui n'est pas en fuite lorsque cela peut faire progresser l'enquête pénale.

Un traitement de données est illicite non seulement en cas d'absence de motifs justificatifs, mais aussi lorsqu'il viole certaines normes juridiques, notamment en cas d'infractions pénales, par exemple en cas de publication de débats officiels secrets (art. 293 du Code pénal; CP) ou de diffamation (art. 173 CP).

L'état de fait visé par l'art. 293 CP est réalisé quand un journaliste, suite à une fuite, rapporte dans son journal les actes confidentiels d'une autorité. Dans ce cas, l'auteur de la publication ne peut en principe invoquer de motifs justificatifs. Toutefois, le journaliste n'est pas punissable s'il pouvait présumer de bonne foi que la personne lui ayant remis les documents a agi dans le cadre de ses compétences, notamment quand les documents n'étaient pas désignés comme confidentiels.

En cas de prévention de diffamation (art. 173 CP), le journaliste peut être libéré de toute responsabilité s'il établit qu'il pouvait considérer comme vraie une fausse affirmation, notamment parce que celle-ci était contenue dans un rapport de police ou provenait d'autres sources pouvant être considérées comme fiables. En outre, le journaliste échappera à toute peine s'il parvient à prouver la vérité de ses allégations.

Cependant, la preuve libératoire n'est pas offerte à celui qui propage des informations sans égard à l'intérêt public et sans autre motif suffisant, essentiellement dans le dessein de dire du mal d'autrui.

En résumé, la publication dans la presse de données anonymes (c'est-à-dire de données ne permettant pas l'identification de la personne concernée) ne constitue pas une atteinte à la personnalité et ne tombe pas dans le champ d'application de la LPD. La publication dans la presse de données personnelles relatives à des enquêtes de police ou à des jugements est licite si elle repose sur un motif justificatif et ne contrevient pas à une norme imposant le secret.

4 Informatique et télécommunication

4.1 Questions relatives à la protection des données liées à l'utilisation de la technologie RFID

Le nombre de domaines dans lesquels on utilise des puces radio est en constante croissance. Ces puces sont capables de lire et de stocker des informations sans nécessiter aucun contact physique, uniquement par transmission d'ondes radio (RFID = Radio Frequency Identification). L'utilisation de puces RFID dans certains domaines ne pose aucun problème alors que dans d'autres domaines elle peut mettre gravement en danger la vie privée de la population. C'est pourquoi des mesures doivent être prises lors de l'application de la technologie RFID pour éviter les traitements illicites de données personnelles.

Une des applications possibles de la technologie RFID est bien connue des citoyens: il s'agit des systèmes anti-vol installés dans les grands magasins. On trouve, aux sorties des magasins, des appareils détecteurs souvent bien visibles qui émettent et reçoivent des signaux radio. La marchandise est, de son côté, munie d'une étiquette contenant une puce RFID (appelée aussi transpondeur ou «tag»). Lorsqu'un client achète un article, le personnel de vente désactive le transpondeur. Si un article avec une étiquette dont le transpondeur n'a pas été désactivé passe devant un lecteur, celui-ci détecte le transpondeur et déclenche une alerte.

Le transpondeur est généralement constitué d'une puce, d'une antenne ainsi que d'un boîtier. Typiquement, les transpondeurs sont intégrés dans des cylindres en verre, des disques ou des cartes en plastique (telles que les cartes EC) ou appliqués sur un film. Ils peuvent être intégrés dans n'importe quel objet ou apposés à celui-ci. La technologie RFID distingue deux types de transpondeurs: les transpondeurs actifs qui disposent de leur propre source d'énergie (pile) et les transpondeurs passifs qui captent l'énergie nécessaire dans les ondes radio émises par le lecteur. C'est avec cette énergie tirée des ondes radio que les transpondeurs passifs sont capables de transmettre les données qu'ils contiennent. La technologie RFID est utilisée notamment dans le domaine de la logistique pour suivre le cheminement de marchandises depuis leur origine à leur destination. On l'utilise par exemple pour l'identification et le suivi des colis dans les entreprises de distribution, pour le marquage de palettes de transport dans les systèmes de gestion d'entrepôts ainsi que pour des opérations d'inventaire. La technologie RFID est également utilisée dans le domaine de la sécurité, par exemple pour l'identification de personnes, d'animaux, de véhicules, pour le contrôle des

accès, la surveillance de marchandises, les systèmes anti-démarrage, les systèmes d'ouverture et de fermeture des portes ainsi que dans le domaine des transports et de la billetterie, par exemple dans les transports publics ou lors de grandes manifestations ainsi que pour les abonnements de ski.

A l'avenir, ce sera vraisemblablement le système de codification EPC (Electronic Product Code), basé sur la technologie RFID, qui fera son entrée dans les grands magasins. Le code EPC est une extension du code à barres actuel, qui utilise le code EAN (European Article Number). L'introduction du code EPC permettra d'identifier de manière univoque chaque objet individuel dans le monde entier. Si un client s'identifie à l'achat de produits (par ex. avec une carte de crédit ou une carte-client), ces identifications uniques d'article pourront lui être attribuées pour une durée prolongée, voire même à vie. Des discussions sont même en cours pour évaluer s'il faut équiper les billets de banque de puces RFID.

Du point de vue de la protection des données, l'utilisation de la technologie RFID présente des dangers puisqu'elle permet, à l'aide d'ondes radio, de traiter des données sur une certaine distance, sans qu'il soit nécessaire d'avoir un contact visuel direct avec la puce et sans que la personne concernée doive activement intervenir dans le processus. Un traitement de données peut donc avoir lieu sans que les personnes concernées s'en rendent compte. Les données contenues dans des transpondeurs RFID qui n'ont pas été effacés ou détruits peuvent être lues à l'aide d'appareils (invisibles). Les données ainsi récupérées peuvent alors être mises en relation, ce qui présente le risque que l'on crée des profils d'achats ou de déplacements.

Le marquage de billets de banque au moyen de puces RFID est également un projet très sensible du point de vue de la protection des données. Nous sommes d'avis qu'il ne doit en aucun cas être possible de retracer quelles personnes ont retiré quels billets de banque à quel distributeur, ni où ces personnes ont acheté quelles marchandises ou prestations de service.

Conformément aux dispositions de la loi sur la protection des données, les données personnelles ne peuvent être traitées que si les personnes concernées ont donné leur accord à ce traitement, à moins que ce dernier ne soit justifié par intérêt prépondérant privé ou public, ou par une base légale. L'accord ne peut être donné que si les personnes concernées ont été informées sur le but du traitement de données et savent quelles données sont traitées quand, où et comment. Le principe de la bonne foi exige en outre que les personnes concernées soient informées de manière transparente.

Nous recommandons aux fabricants et exploitants d'applications ou de systèmes utilisant la technologie RFID de prendre les mesures nécessaires pour garantir que celle-ci sera utilisée en conformité avec les exigences de la protection des données. Il convient d'attacher une attention particulière aux points suivants:

- Le traitement de données personnelles doit être évité dans la mesure du possible. S'il est inévitable, les personnes concernées doivent être informées clairement et de manière transparente sur la finalité du traitement de données ainsi que sur le système d'information. En plus de l'indication du but du traitement, il y a lieu de préciser également quelles sont les données saisies, comment celles-ci sont traitées (par ex. à qui elles sont communiquées) et quand elles sont supprimées. Un premier pas en direction d'une certaine transparence consiste à indiquer aux clients quels produits sont équipés d'étiquettes RFID.
- Les données collectées doivent être utilisées uniquement pour le but annoncé.
- Le droit d'accès doit être garanti.
- Les transpondeurs doivent, selon leur utilisation, être détruits ou désactivés et les données qu'ils contiennent doivent pouvoir être supprimées. Si une personne vient à posséder des puces RFID, par exemple à la suite d'un achat ou par transmission d'un objet d'une personne à une autre, elle doit avoir la possibilité de supprimer ou de faire supprimer les données, intégralement ou partiellement, pour éviter que celles-ci puissent être reconstruites. La personne doit en outre avoir également la possibilité de détruire ou de faire détruire la puce. Lors d'un prêt de produits (par ex. prêt de livres dans une bibliothèque), il faut veiller à ce que les transpondeurs soient désactivés lors de l'opération de prêt afin d'éviter que leur contenu puisse être lu pendant qu'ils se trouvent en possession de l'utilisateur. Le transpondeur ne devra être réactivé qu'une fois que la marchandise aura été retournée.
- La sécurité des informations doit être assurée: les systèmes doivent être conçus de manière à être sûrs et doivent en particulier garantir la confidentialité, la disponibilité et l'intégrité des données. Les informations contenues dans les puces RFID doivent être protégées (par ex. par des procédés de cryptage) de manière à ce qu'elles soient accessibles uniquement pour l'application prévue. Le détenteur d'un appareil de lecture/écriture ne doit pas être en mesure d'extraire des informations d'une puce RFID non protégée. Un scénario très dangereux se présenterait si une personne équipée d'un appareil lecteur réussissait à découvrir quelle somme d'argent une personne porte sur soi.

4.2 Enregistrement des cartes SIM à prépaiement pour téléphones mobiles

En août 2004 est entrée en vigueur une disposition obligeant les fournisseurs de services de téléphonie mobile à enregistrer les acheteurs de cartes SIM à prépaiement. L'efficacité de cette action très coûteuse reste cependant douteuse.

En automne 2003, les Chambres fédérales ont accepté un complément à la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, en discussion depuis plusieurs années déjà. La disposition oblige les acheteurs de cartes SIM à prépaiement à décliner leur identité. L'objectif de cette mesure est de pouvoir mieux lutter contre la criminalité. Les fournisseurs de services de télécommunication sont tenus de conserver ces données pour une durée de deux ans au moins. Ces données ne sont nécessaires ni pour la fourniture de la prestation, ni pour la facturation.

Les dispositions concernant l'obligation de s'enregistrer sont entrées en vigueur le 1er août 2004. Celles-ci prévoient l'enregistrement de tous les nouveaux clients ainsi que des clients existants ayant mis en service leur carte dès le 1er novembre 2002. Les cartes plus anciennes peuvent continuer à être utilisées sans être enregistrées. Les opérateurs doivent s'assurer, lors de la vente de cartes SIM à prépaiement, que les nom, prénom, adresse et date de naissance sont saisis sur la base d'un passeport valable, d'une carte d'identité ou d'un autre document de voyage reconnu pour l'entrée en Suisse. Ils doivent en outre noter le type et le numéro du document présenté.

Un fournisseur de services de téléphonie mobile prévoyait d'utiliser les données collectées au moyen de ce formulaire d'enregistrement à d'autres fins que celles prévues dans la base légale. Une telle utilisation nécessite cependant l'accord préalable de la personne concernée. Or, les clients n'étaient pas clairement informés de la possibilité de ne pas fournir ces autres données. Suite à notre intervention, le formulaire a par la suite été adapté en conséquence. Il indique maintenant clairement quelles données doivent être obligatoirement fournies et celles qui sont facultatives, respectivement quels traitements de données doivent être effectués.

La transmission de la carte SIM de l'acquéreur initial à une autre personne n'est pas soumise à la déclaration obligatoire. Ceci serait d'ailleurs difficile à mettre en œuvre. Cela signifie donc que la personne qui utilise la carte n'est pas forcément la même que celle qui a été enregistrée au moment de la vente de la carte. En outre, il est toujours possible de téléphoner en Suisse avec des cartes à prépaiement qui ont été délivrées par des opérateurs étrangers et ne sont donc pas enregistrées. Vu ces possibilités de contournement de la loi, il paraît donc douteux qu'un tel enregistrement permette de combattre efficacement la criminalité et le terrorisme. Par contre, ces données collectées sur des centaines de milliers de personnes présentent un certain risque de violation de la protection des données.

4.3 Communication de données personnelles lors de l'encaissement de services à valeur ajoutée dans le domaine des télécommunications

Les services à valeur ajoutée dans le domaine des télécommunications sont en général facturés aux clients par l'entreprise de télécommunication. Les fournisseurs de services à valeur ajoutée n'ont ainsi aucun accès aux données des clients. Si le client conteste avoir eu recours au service qui lui est facturé, la question se pose de savoir si et sous quelle forme ces données peuvent être transmises aux fournisseurs de services à valeur ajoutée afin de leur permettre un encaissement direct. Nous avons examiné si ce genre de communication des données personnelles est licite du point de vue de la protection des données.

La loi sur la protection des données (LPD) exige d'une manière générale la présence d'un motif justificatif pour le traitement de données personnelles; cela peut être le consentement de la personne concernée, une disposition légale ou un intérêt public ou privé prépondérant.

Le fait de s'opposer à la facturation des services à valeur ajoutée pourrait être considéré comme un consentement à la communication des données personnelles dans la mesure où les conditions générales de l'entreprise de télécommunication sont suffisamment transparentes. Un tel consentement n'équivaut toutefois pas à un libre choix car la seule alternative possible dans ce cas est de payer le montant litigieux. Il n'existe pas de disposition légale qui requiert ou admet expressément la communication des données des clients au fournisseur de services à valeur ajoutée. Aucun intérêt public prépondérant ne saurait davantage entrer en considération.

Néanmoins, la LPD énumère, dans une liste non exhaustive, les cas dans lesquels on part du principe qu'il existe un intérêt prépondérant de la personne qui traite des données personnelles. Ceci peut notamment être le cas lorsque le traitement est en relation directe avec la conclusion ou l'exécution d'un contrat et les données traitées concernant le cocontractant. En cas de recours à des services à valeur ajoutée, un contrat est conclu d'une part entre le client et l'entreprise de télécommunication et d'autre part entre le client et le fournisseur de services à valeur ajoutée. Dans ce cas, on peut dire que le fournisseur de services à valeur ajoutée dispose d'un intérêt prépondérant pour traiter ces données.

Cela dit, il convient de veiller dans chaque cas au respect des principes généraux posés par la LPD pour le traitement des données. En particulier, le principe de la proportionnalité exige que le traitement ne porte que sur les données qui sont néces-

saires et aptes à atteindre le but visé. Dans le cas d'espèce, cela signifie que l'entreprise de télécommunication ne doit communiquer que les données dont le fournisseur de services à valeur ajoutée a besoin pour le recouvrement de ses créances, à savoir le nom, l'adresse et le montant dû.

Toutefois, si le client conteste avoir eu recours à la prestation en connaissance de cause (par ex. dans le cas des dialers Internet), la réalisation d'un contrat entre l'appelant et le fournisseur de services à valeur ajoutée est litigieux. Dans un tel cas, il convient que les clients et les fournisseurs de services à valeur ajoutée prennent directement contact afin de déterminer si le contrat est valable. Comme il est de l'intérêt des clients de pouvoir contester l'existence d'un contrat valable, rien ne s'oppose, du point de vue de la protection des données, à la communication des données de ces clients.

Il convient d'examiner encore si une telle communication est également conforme aux dispositions spéciales du droit des télécommunications.

Le secret des télécommunications – qui est un droit fondamental inscrit dans la Constitution- protège en premier lieu le contenu des communications. Mais cette protection s'étend aussi à toutes les autres informations personnelles relatives aux communications. La loi sur les télécommunications dispose qu'il est interdit aux fournisseurs de services de télécommunication de transmettre à des tiers des renseignements sur les communications des usagers. Le prestataire de services à valeur ajoutée est, en qualité d'interlocuteur appelé, considéré comme un tiers. L'interdiction de renseigner faite à l'entreprise de télécommunication peut être levée lorsque les données personnelles («noms et adresses des abonnés dont les raccordements ont servi à établir ces communications») sont requises pour identifier les communications établies de manière abusive (par ex. les harcèlements téléphoniques) ou encore, selon la disposition du code pénal concernant la violation du secret des postes et des télécommunications (art. 321ter CP), pour «déterminer l'ayant droit ou pour prévenir la survenance de dommages». Dans le cas d'espèce, on ne peut faire valoir une telle exception, du moins pour le prestataire de services à valeur ajoutée.

Dans ces conditions, nous estimons qu'il est nécessaire de créer une base légale dans la loi sur les télécommunications; toutefois, il faudrait tout d'abord examiner attentivement s'il s'agit d'une lacune juridique – une inconséquence de la loi – ou un silence qualifié du législateur. Du point de vue de la protection des données, rien ne s'oppose à la création d'une telle base légale dans la loi sur les télécommunications.

5 Santé

5.1 Thèmes divers

5.1.1 Questions relatives à la protection des données en rapport avec le tarif médical Tarmed

En prévision de l'entrée en vigueur au 1er janvier 2004 du tarif médical Tarmed pour le domaine de la LAMal, nous avons procédé à deux examens des faits. Les résultats ont démontré que, tel qu'il est pratiqué actuellement, le traitement systématique de données personnelles est disproportionné. Il incombe aux acteurs impliqués d'élaborer des solutions qui prennent en compte les exigences de la protection des données.

La convention-cadre Tarmed règle une structure tarifaire commune ainsi qu'une procédure uniforme de remboursement entre ceux qui fournissent les prestations et ceux qui en supportent les coûts. L'introduction de Tarmed prévoit qu'après une période de transition de deux ans, la facturation entre fournisseurs de prestations et organismes payeurs soit effectuée de manière électronique. Le passage de la facture imprimée au formulaire de facturation électronique facilitera les contrôles systématiques. Si les mesures nécessaires ne sont pas prises, le risque d'atteinte à la protection de la personnalité augmente. Nous avons par le passé attiré à plusieurs reprises l'attention sur les risques pour la protection des données liés à l'introduction du tarif médical Tarmed (cf. 10ème rapport d'activités 2002/2003, chiffre 5.1.5; 9ème rapport d'activités 2001/2002, chiffre 5.1.4; 8ème rapport d'activités 2000/2001, chiffre I 7.5).

Selon la loi, le fournisseur de prestations doit remettre au débiteur une facture détaillée et compréhensible. L'assureur peut demander un diagnostic précis ou des informations complémentaires de nature médicale. En outre, le fournisseur de prestations est autorisé, lorsque les circonstances l'exigent, ou obligé si l'assuré le demande, à ne fournir les indications d'ordre médical qu'au médecin-conseil de l'assureur.

A l'article 42 al. 3 et 4 de la Loi fédérale sur l'assurance-maladie (LAMal), le législateur prévoit une communication échelonnée par le fournisseur des prestations des données relatives au traitement. L'assureur peut exiger des renseignements supplémentaires en complément des indications reçues. Le législateur exclut par conséquent qu'une communication systématique, sous forme détaillée, de diagnostics et de données relatives aux traitements médicaux aie lieu dans une première étape déjà. La communication systématique de diagnostics ou de codes de diagnostic aux assureurs est non seulement contraire au principe de proportionnalité ancré dans la loi

fédérale sur la protection des données, mais il viole également l'art. 42 LAMal. Le principe de la proportionnalité ne permet de récolter que les données vraiment nécessaires et aptes à atteindre le but poursuivi. Une importance accrue doit être accordée au respect de ce principe en présence de données sensibles.

Les examens des faits (cf. notre rapport «Tarmed et la protection des données» du 22 juin 2004, http://www.edsb.ch/f/themen/gesundheit/tarmed-bericht_f.pdf) ont révélé que les assureurs doivent selon la loi remplir plusieurs tâches différentes. Ceux-ci doivent notamment vérifier la prise en charge de la prestation par l'assurance-maladie, le caractère économique des prestations fournies par les médecins, ainsi que la facture à payer. Les besoins en données ne sont pas les mêmes pour chacune des ces tâches. Les assureurs n'ont pas besoin de toutes les données concernant une personne. Il y a donc lieu de veiller à ce que, pour chaque étape de travail, seules les données qui sont appropriées et absolument nécessaires soient transmises. Pourtant, les données exigées sur le formulaire de facturation couvrent l'ensemble des informations disponibles sur une personne. Le traitement sous cette forme n'est, dans ces conditions, pas proportionnel.

La législation prescrit que soit élaboré un règlement de traitement qui définisse les mesures techniques et organisationnelles permettant d'assurer un traitement des données qui soit conforme aux exigences de la protection des données. Le règlement de traitement doit en particulier définir les délais de conservation, le type et l'étendue de l'accès que les utilisateurs ont aux fichiers, les procédures à suivre pour la rectification, le blocage et l'anonymisation ou la pseudonymisation.

Nous sommes d'avis qu'il faut élaborer, en complément au règlement de traitement, un concept de protection des données; en effet, le traitement systématique de données des patients exige une description détaillée des mesures conceptuelles permettant de réduire à un minimum le risque d'une atteinte à la personnalité. Ce concept doit également permettre aux personnes concernées d'être informées de manière claire sur la nature des traitements de données effectués. Le règlement de traitement et le concept de protection des données doivent régulièrement être contrôlés par le maître de fichier quant à leur application et leur actualité.

5.1.2 Surveillance du respect des charges assorties aux autorisations accordées dans le domaine de la recherche médicale

La Commission d'experts du secret professionnel en matière de recherche médicale délivre des autorisations pour des projets de recherche. La tâche du PFPD consiste à vérifier que les conditions liées à ces autorisations sont respectées. Nous avons vérifié le respect des conditions assorties pour deux autorisations et avons communiqué le résultat de notre enquête dans un rapport adressé à la Commission d'experts.

La Commission d'experts du secret professionnel en matière de recherche médicale a pour tâche de délivrer, sous certaines conditions, des autorisations pour des projets de recherche. La commission d'experts a une composition paritaire: la recherche, l'association des médecins et les organisations de patients y sont représentés chacun par 3 membres; à ceux-ci s'ajoutent deux juristes. La Commission d'experts est soumise à la surveillance du Conseil fédéral auquel elle doit périodiquement rendre compte de son activité. Les détails sont réglés dans l'Ordonnance concernant les autorisations de lever le secret professionnel en matière de recherche médicale (OALSP).

La Commission délivre des autorisations pour des projets de recherche isolés (autorisations particulières), pour des hôpitaux (autorisations générales, appelées aussi «autorisations de cliniques») ainsi que pour des registres médicaux dans le domaine de la recherche médicale, comme par exemple le registre du cancer (autorisations générales également). Ce sont des questions de protection des données qui se posent, en particulier la question de la communication et de l'utilisation de données concernant le patient à des fins de recherche médicale.

Les autorisations particulières doivent être limitées au projet de recherche mentionné dans la demande. Toute modification du projet de recherche, notamment de son but, doit faire l'objet d'une nouvelle demande d'autorisation. Les autorisations générales octroyées aux cliniques et aux instituts médico-universitaires permettent au personnel chargé de recherches internes ainsi qu'aux candidats au doctorat d'accéder à des données personnelles, pour autant que les intérêts légitimes des intéressés ne soient pas compromis et que les données soient rendues anonymes dès le début des recherches.

La Commission d'experts peut octroyer aux organes responsables de registres médicaux utilisés à des fins de recherche médicale des autorisations générales les habilitant à recevoir des données qui n'ont pas été rendues anonymes.

L'octroi de telles autorisations est, selon l'art. 321bis du Code pénal (CP), soumis à des conditions cumulatives strictes: L'autorisation ne peut être délivrée que si l'intéressé, après avoir été informé de ses droits, n'a pas expressément refusé son consentement, si la recherche ne peut être effectuée avec des données anonymes, s'il est impossible ou particulièrement difficile d'obtenir le consentement de l'intéressé ou si les intérêts de la recherche priment l'intérêt au maintien du secret.

L'octroi de l'autorisation n'engendre aucune obligation de communiquer des données; elle en confère uniquement le droit (cf. à ce propos notre 3ème rapport d'activités 1995/1996, chiffre 6.1, ainsi que notre 5ème rapport d'activités 1997/1998, chiffre 6.1).

Une fois que la commission a autorisé la levée du secret professionnel, le PFPD a pour tâche de surveiller le respect des charges qui sont assorties à cette autorisation, notamment en ce qui concerne la sécurité des données.

Cette année, nous avons vérifié le respect des charges pour une autorisation particulière ainsi que pour une autorisation générale (autorisation de clinique). Les charges sont des mesures permettant de protéger et de maintenir la sécurité des données communiquées. Ainsi, les données doivent être anonymisées le plus tôt possible. D'autre part, les données non anonymisées se présentant sous forme papier doivent être gardées sous clé et celles qui sont enregistrées sur des supports électroniques doivent être protégées par un mot de passe. Cette mesure permet de délimiter le cercle des personnes autorisées à accéder à ces données. Seuls les détenteurs de l'autorisation ainsi que leurs assistants sont autorisés à accéder aux données non anonymisées.

Pour notre examen, nous avons consulté des autorisations de la Commission d'experts et en avons sélectionné deux pour nos contrôles. Nous avons ensuite demandé aux chercheurs de nous fournir les documents relatifs à l'exécution du projet de recherche ainsi qu'au traitement de données s'y rapportant. Dans une étape suivante, nous avons analysé les documents reçus puis élaboré un questionnaire. Après cela, nous avons demandé à assister sur place à un traitement de données.

Notre contrôle a révélé que les charges ont en principe été respectées. Nous avons communiqué les résultats de nos contrôles à la Commission d'experts sous forme de rapport.

Nous prévoyons à l'avenir de procéder à d'autres contrôles, ceci en étroite collaboration avec la Commission d'experts, afin de vérifier que les charges sont bel et bien respectées et nous allons continuer à conseiller la Commission d'experts pour les questions de protection des données.

5.2 Génétique

5.2.1 Loi fédérale sur l'analyse génétique humaine

En octobre 2004, le parlement a approuvé la loi fédérale sur l'analyse génétique humaine. La loi contient notamment de nombreuses dispositions sur la protection de la personnalité.

Le délai référendaire concernant la loi fédérale sur l'analyse génétique humaine (LAGH) est arrivé à échéance le 27 janvier 2005. La LAGH, ainsi que les dispositions d'exécution y relatives entreront probablement en vigueur au milieu de l'année 2006.

Le champ d'application de la LAGH couvre les analyses génétiques dans les domaines médical, du travail, des assurances et de la responsabilité civile. En outre, la LAGH régit l'établissement de profils d'ADN dans le but de déterminer la filiation ou d'identifier des personnes (cf. également notre 10ème rapport d'activités 2002/2003, chiffre 5.2.2).

Selon cette loi, nul ne doit être discriminé en raison de son patrimoine génétique. Les analyses génétiques et prénatales ne peuvent être effectuées que si la personne concernée a donné son consentement libre et éclairé. Par ailleurs, toute personne peut refuser de prendre connaissance d'informations relatives à son patrimoine génétique (droit de ne pas savoir). Les analyses génétiques sont soumises à l'autorisation de l'autorité fédérale compétente.

Dans le cadre des analyses génétiques, la personne concernée doit bénéficier de conseils fournis par un personnel disposant des connaissances requises. Elle doit notamment être informée des buts, des risques, des répercussions physiques et psychiques éventuelles d'une analyse. Le principe de transparence exige que la personne concernée soit informée de manière complète.

Les analyses génétiques sont interdites dans le domaine du travail, de l'assurance et de la responsabilité civile, ainsi que si elles ont pour but de déterminer la filiation. Néanmoins, des exceptions sont prévues si certaines conditions sont remplies. Par exemple, les analyses génétiques sont en principe autorisées pour les assurances sur la vie dont la somme assurée est supérieure à 400'000 francs.

Du point de vue de la protection des données, la LAGH peut être qualifiée de réussite et tient également compte du droit de la personne concernée de disposer librement des informations la concernant. Reste à savoir si et comment la loi sera appliquée. Mentionnons enfin que la LAGH tient également compte de l'évolution internationale, en particulier du protocole du Conseil de l'Europe sur la génétique humaine dont les travaux sont sur le point d'être achevés (pour plus de détails à ce propos, se reporter à notre 11ème rapport d'activités 2003/2004, chiffre 11.1.1.).

6 Assurances

6.1 Assurances sociales

6.1.1 Lacunes des réglementations dans le domaine de la protection des données médicales

L'Office fédéral des assurances sociales (OFAS) nous a invités à nouveau à nous prononcer sur le rapport concernant la protection des données médicales dans le domaine des assurances sociales. Toutefois, notre avis n'a été pris en considération que sur certains points.

Un rapport a été établi suite au postulat de la Commission des affaires juridiques du Conseil national (99.093) qui demandait un «rapport englobant tous les domaines des assurances sociales et qui porte sur les lacunes qui existent en matière de protection des données médicales». Ce rapport devait tenir compte de l'évolution technologique du traitement électronique des données ainsi que des dangers d'abus qui en découlent. Les réflexions devaient inclure la protection du secret médical prévu par l'article 321 du Code pénal.

L'OFAS nous a invités cette année encore à remettre notre prise de position à ce sujet (cf. également le 11ème rapport d'activités 2003/2004, chiffre 6.1.1). Les divergences entre l'OFAS et le PFPD n'ont toutefois pas pu être éliminées sur des points essentiels.

Dans nos différentes prises de position, nous avons relevé que le rapport allait dans la bonne direction et qu'il donnait une bonne vue d'ensemble sur les lacunes en matière de réglementation dans le domaine de la protection des données médicales. Le rapport souligne tout particulièrement les lacunes en matière d'exécution. Il reconnaît par exemple de manière pertinente qu'il faut améliorer la transparence du traitement des données pour les personnes assurées. Ceci vient corroborer la position du PFPD qui, depuis des années, attire l'attention sur la situation critique qui règne en matière d'exécution des mesures de protection des données dans le domaine des assurances sociales.

Par contre, le rapport ne comporte ni propositions de solution, ni mesures concrètes sur la manière de combler les lacunes et de remédier à cette situation critique. Nous avons fait des propositions à l'OFAS dans ce sens. Il serait par exemple envisageable de prévoir dans la législation relative au domaine des assurances sociales des procédures de certification de protection des données. Enfin, nous avons prié l'OFAS de soumettre notre prise de position au Conseil fédéral.

6.1.2 La 5ème révision de l'assurance-invalidité

Nous avons eu l'occasion de nous prononcer sur la 5ème révision de l'AI dans le cadre de la consultation des offices. Une collaboration renforcée de tous les protagonistes devrait permettre de freiner l'augmentation du nombre des nouvelles rentes. Ce projet soulève toutefois des questions en matière de protection des données.

Le projet de loi prévoit notamment des mesures devant permettre le maintien des personnes assurées dans la vie professionnelle, ce qui implique une collaboration renforcée entre l'employeur, l'assureur d'indemnités journalières et l'office AI. L'une de ces mesures prévoit la création de centres spéciaux indépendants chargés de la détection et du suivi des personnes atteintes dans leur santé (ci-après: centres DPS). Ces centres DPS ont pour but d'effectuer des études complètes afin de clarifier la situation en matière médicale, sociale et professionnelle de la personne assurée. Ces études impliquent le traitement de nombreuses données personnelles.

Nous avons souligné, dans le cadre de la consultation des offices, que le traitement de données personnelles sensibles (données médicales) nécessitait une base légale au sens formel. Il convient en particulier de fixer l'étendue et le but du traitement des données dans une base légale claire.

Par ailleurs, les principes de la protection des données doivent être respectés. Le principe de la proportionnalité, par exemple, requiert que seules les données personnelles appropriées (aptes à atteindre le but poursuivi) et nécessaires puissent être traitées. La situation est très délicate à cet égard lorsque l'employeur doit participer aux études mentionnées ci-dessus. Aujourd'hui déjà, il y a une forte tendance à considérer l'employé (malade) uniquement comme un facteur de coûts. On ne peut écarter le risque de discrimination puisque ni le droit des obligations, ni le présent projet de loi ne prévoient dans ce cas une protection expresse contre le licenciement.

En outre, le traitement de données doit être transparent pour la personne assurée (cf. art. 4, al. 2, LPD). Ce principe s'applique en particulier au traitement de données sensibles concernant l'état de santé psychique (selon le projet de message, l'augmentation des rentes nouvellement accordées est due à l'augmentation des cas de troubles psychiques). Le projet de loi prévoit effectivement que les centres DPS sont tenus d'informer les personnes concernées au préalable et de manière complète sur le but et l'ampleur du traitement des données.

On ne peut dire, à l'heure actuelle, si et dans quelle mesure le projet de loi respecte les droits de la personnalité des travailleurs. En effet, les procédures ne sont pas encore claires sur tous les points et de nombreuses questions sont encore en suspens. Nous continuerons de suivre les nouveautés de la 5ème révision de l'AI et les examinerons sous l'angle de leur conformité avec la protection des données.

6.1.3 Révision de la Loi fédérale sur l'assurance-maladie

Après l'échec de la seconde révision de la LAMal, le Conseil fédéral a décidé de scinder le projet de révision en deux paquets législatifs contenant chacun plusieurs messages. Ils nous ont été soumis pour que nous nous prononcions à leur sujet. Deux points sont à relever sous l'angle de la protection des données: l'introduction de la carte d'assuré et les systèmes de *managed care*.

En octobre 2004, le parlement a adopté les bases légales permettant de créer une carte d'assuré. Le Conseil fédéral est donc en mesure d'introduire une carte d'assuré dans le domaine de la LAMal. Par ailleurs, le Conseil fédéral est chargé de s'occuper de la sécurité des données, et de régler en particulier l'étendue du traitement des données, ainsi que les droits d'accès. Outre des données administratives, la carte d'assuré devra également contenir le nouveau numéro d'assurance sociale (voir également notre 10ème rapport d'activités 2002/2003, chiffre 6.1.3). De plus, des données d'urgence pourront également y être intégrées, à condition que la personne assurée donne son consentement. A long terme, la tendance est de faire évoluer cette carte vers la carte de santé. Actuellement, le Conseil fédéral et l'Office fédéral de la santé publique élaborent un concept de mise en œuvre pour la carte d'assuré, comprenant l'organisation du projet. Nous suivons ce projet sous l'angle de la protection des données.

Le second paquet législatif prévoit les systèmes de *managed care*. Concrètement, il est prévu d'introduire dans la loi des modèles d'assurance avec réseaux de soins intégrés. Les modèles de *managed care* ont pour objectif de garantir aux assurés des soins de bonne qualité et d'endiguer les coûts de la santé.

On peut saluer le fait que la personne assurée puisse décider librement si elle veut ou non participer à ces nouveaux modèles. Ceci correspond au libre choix du citoyen en matière d'information, à savoir le droit pour la personne assurée de décider librement du traitement des données la concernant.

Il est également prévu que l'échange de données entre les services concernés sera réglé par contrat. Néanmoins, si des données personnelles sont traitées dans le cadre des modèles de *managed care*, les contrats ne sont en principe pas suffisants et il faut créer les bases légales nécessaires.

Toutefois, le projet de loi n'est pas suffisamment clair en ce qui concerne les différents processus d'information; en effet, ni le projet de loi, ni le message ne précisent le contenu des nouvelles formes particulières d'assurance et des traitements de données. Il est donc impossible, dans l'état actuel des choses, d'apprécier les modèles de *managed care* sous l'angle de la protection des données.

6.2 Assurances privées

6.2.1 Lutte contre l'abus en matière d'assurances et protection des données

Les assurances privées qui prennent des mesures contre l'abus en matière d'assurances sont soumises à la législation sur la protection des données. Un cas a donné lieu à un examen approfondi de la situation par le PFPD.

Les assureurs privés sont de plus en plus nombreux à prendre des mesures contre l'abus à l'assurance. Ils sont néanmoins tenus, dans chaque cas, de tenir compte des principes de la protection des données. Au cours de la période étudiée, nous avons poursuivi et achevé l'examen d'un cas concernant un assureur privé (se reporter également à notre 11ème rapport d'activités 2003/2004, chiffre 6.2.2.).

Il s'est agi en l'occurrence de deux fichiers internes automatisés d'un assureur privé qui n'avaient pas été annoncés au PFPD (cette lacune a été comblée dans le cadre des mises au point effectuées par le PFPD). Ces deux fichiers ont pour but de lutter contre l'abus et la fraude à l'assurance. Ils contiennent notamment des données relatives au cas traité, des remarques, des indications concernant l'identité des assurés, ainsi que d'autres personnes impliquées, de même que des données sur d'éventuelles procédures pénales et civiles. Ces fichiers contiennent donc des données sensibles, voire même des profils de la personnalité. Ils touchent d'une part au domaine des assurances privées, d'autre part aux domaines de la LAMal et de la LAA.

Voici les conclusions auxquelles nous sommes parvenus:

Les deux fichiers sont soumis à l'obligation de déclaration et auraient dû être déclarés au PFPD immédiatement lors de leur mise en exploitation. Cela a été fait trop tard. Par

ailleurs, nous avons proposé de rendre le traitement des données plus transparent pour les personnes assurées. On pourrait par exemple envisager d'introduire, dans le cadre de la procédure de demande d'affiliation, une fiche donnant aux assurés des informations détaillées sur le traitement des données en relation avec l'abus d'assurance. Une meilleure transparence correspond également aux tendances observées au niveau international; il convient à ce propos de rappeler l'existence de la Recommandation Rec(2002)9 du Conseil de l'Europe sur la protection des données à caractère personnel collectées et traitées à des fins d'assurance (voir également la révision en cours de la LPD ainsi que les révisions terminées de la LCA et de la LSA; à ce sujet, voir notre 11ème rapport d'activités 2003/2004, chiffre 6.2.3).

Par ailleurs, nous avons constaté que la base légale pour la collecte des données dans le domaine de l'assurance-maladie et de l'assurance-accidents obligatoire n'était pas suffisante. En effet, les données personnelles sensibles et les profils de la personnalité ne peuvent en principe être traitées par l'assureur social que si une loi au sens formel le prévoit (cf. art. 17 LPD). A notre avis, il n'existe ni dans la LAMal, ni dans la LAA une base légale suffisante permettant la tenue systématique d'une «banque de données des cas de fraude».

Enfin, nous avons prié l'assureur de garantir la transparence des différents processus d'information et d'élaborer un règlement de traitement pour les fichiers cités plus haut. L'assureur privé a élaboré un règlement de traitement et communiqué son intention d'effectuer un contrôle périodique (audit) avec le concours du responsable de la sécurité informatique.

7 Secteur du travail

7.1 La journalisation des activités à la caisse pour examiner les différences d'inventaires

La journalisation systématique des activités à la caisse ne doit être effectuée que si certaines conditions sont remplies. Il doit y avoir un risque de dommage financier pour l'employeur en raison d'un vol, d'une fraude ou d'une erreur de manipulation à la caisse. Les personnes concernées doivent être informées à l'avance. Dans le cas où les activités à la caisse sont examinées en raison d'un éventuel abus ou d'une erreur de manipulation, il faut traiter les données personnelles sous une forme pseudonymisée. Si l'on constate des comportements irréguliers, les personnes concernées pourront alors être identifiées.

Une entreprise de dimension mondiale nous a contactés pour savoir si la journalisation systématique des activités de ses employés à la caisse était légale. La question avait essentiellement pour objectif de savoir si une telle pratique enfreignait la loi sur la protection des données et la législation sur le travail. L'entreprise a précisé que l'objectif premier de la journalisation était de sauvegarder systématiquement des preuves permettant de faire la lumière sur les différences d'inventaires causées intentionnellement ou par négligence. Les informations ainsi rassemblées feraient l'objet de recherches en cas de comportements irréguliers. En cas de détection d'une irrégularité, de plus amples recherches seraient entreprises, le cas échéant en les ciblant sur certains collaborateurs. Des analyses plus précises ne ne devraient être établies qu'en cas de découverte d'activités incorrectes ou frauduleuses.

Nous avons communiqué à l'entreprise ce qui suit:

Les données traitées par la journalisation comprennent toute une série d'activités à la caisse, allant de la connection ou de la déconnection de l'utilisateur aux paiements par cartes de crédit, en passant par les achats des collaborateurs ou le règlement d'achats à l'aide de bons. En plus de la prestation (par ex. la rapidité à la caisse) et, cas échéant, un comportement délictueux, un tel traitement de données permet également de constater les absences au poste de travail, les achats personnels, etc. Les informations traitées constituent des données personnelles au sens de la loi sur la protection des données, les employés concernés étant des personnes déterminés ou déterminables. Les moyens de preuve relatifs à un comportement délictueux sont des données sensibles au sens de la LPD (données concernant les poursuites et les sanctions pénales) et doivent ainsi bénéficier d'une protection particulière. L'ensemble des données relatives aux prestations et au comportement d'un employé peut même constituer un profil de la personnalité.

La journalisation est en principe justifiée dans la mesure où il existe pour l'employeur un risque de dommage financier en raison d'un vol, d'une fraude ou d'une erreur de manipulation involontaire à la caisse et qu'il n'y a pas d'autres mesures moins incisives permettant d'atteindre le même but. Dans ce contexte, et conformément au principe de proportionnalité, il convient de d'empêcher – si possible dès le début – les abus ou les erreurs de manipulation involontaires, en mettant en place des mesures techniques ou organisationnelles. De plus, seules les données en relation avec des noms de personne se rapportant à des cas d'abus ou de manipulations erronées peuvent être traitées. Les autres données saisies concernant le comportement professionnel ou privé (par ex. absences personnelles, achats particuliers, etc.) des employés ne sauraient être exploitées. La durée de conservation doit également être fixée selon le principe de la proportionnalité ; un délai d'un à deux mois semble suffisant pour détecter des pratiques suspectes ou des erreurs de manipulation à la caisse.

Le maître du fichier doit informer ses employés au préalable de la mise en œuvre de la journalisation. D'une part, il doit leur expliquer la finalité et les fonctions de la journalisation, d'autre part les informer sur les effets d'un traitement de données personnelles, les catégories de personnes ayant accès à ces données, la durée de conservation ainsi que surle droit d'obtenir des renseignements (droit d'accès).

Pour ce qui est de la sécurité des données, il convient de protéger le serveur afin d'empêcher l'accès des personnes non autorisées. Les accès doivent être limités aux personnes chargées de procéder à l'exploitation des données et aux catégories de données qui sont absolument nécessaires à l'examen des différences d'inventaires. L'échange de données avec d'autres serveurs n'est en principe pas admis. Le local des serveurs doit être protégé contre l'accès de tiers non autorisés par des mesures techniques et organisationnelles.

La surveillance systématique ciblée du comportement des employés étant en principe interdite, ce genre de contrôle des activités de caisse ne doit avoir lieu que sur la base de données personnelles pseudonymisées. Les personnes ne doivent être identifiées qu'en cas d'irrégularités flagrantes. Dans ces conditions, la journalisation des activités de caisse porte certes une atteinte (légère) à la personnalité des employés mais, sous l'angle de la proportionnalité, elle peut être considérée comme compatible avec la loi sur la protection des données (LPD).

7.2 Le contrôle des présences à l'aide des empreintes digitales

Le contrôle des présences au poste de travail s'effectue aujourd'hui de plus en plus à l'aide de logiciels de traitement des empreintes digitales. Si le stockage centralisé des empreintes digitales est problématique au niveau de la protection des données, celui des seules minuties associées à l'identité l'est beaucoup moins, à condition toutefois que des mesures de sécurité soient appliquées. Toutefois, la solution du stockage des données biométriques dans une carte à puce à usage exclusif, présentée par chaque employé lors du timbrage, représente une solution plus proportionnée et donc conforme à la législation sur la protection des données.

Une entreprise active dans la région genevoise nous a soumis la question de la compatibilité du traitement d'empreintes digitales pour le contrôle des présences avec la protection des données. Il s'agissait en particulier d'examiner si le recours à la biométrie est justifié et proportionné au regard de l'objectif poursuivi. Nous sommes arrivés aux conclusions suivantes:

Le contrôle des présences et des accès au poste de travail s'effectue aujourd'hui de plus en plus à l'aide de logiciels. Ces logiciels peuvent s'intégrer dans les environnements bureautiques, permettant parfois même la consultation de leurs données par d'autres logiciels. Les logiciels de gestion des présences, dont les accès sont généralement protégés par des mots de passe, peuvent saisir, outre les catégories de données classiques (nom, prénom, département ou unité, adresse, horaires de travail, etc.), les opérations ou les mouvements particuliers (accès à l'intérieur de l'entreprise, utilisation de véhicules, etc.) Avec certains logiciels, le traitement des données est effectué au moyen des empreintes digitales des employés. Dans une première phase, l'empreinte du doigt est numérisée et analysée afin d'en extraire les minuties, c'est-à-dire certaines caractéristiques du doigt, telles que les endroits où apparaît une bifurcation ou une terminaison des crêtes et les sillons tracés sur la surface du doigt. Ensuite vient la phase d'authentification, durant laquelle le système autorise ou refuse l'accès, selon le résultat de la comparaison des minuties du doigt présenté avec l'échantillon de référence. En principe, l'*authentification* seule peut suffire à accorder l'accès requis à une personne qui conserve alors son anonymat. Dans le cas du pointage des présences, l'*identification* des personnes est par contre nécessaire. Pour ce faire, nous recommandons l'usage d'un identifiant présenté par chaque employé lors du timbrage, plutôt qu'une comparaison sur la base d'une collection centralisée de minuties de référence associées aux identités correspondantes.

Les empreintes digitales, de même que les minuties qui en sont extraites, représentent des données biométriques statiques. Elles ne varient pas au cours du temps et sont inhérentes à la personne concernée, en manifestent l'originalité et ne peuvent en principe être usurpées. Sans association avec l'identité, les éléments biométriques ne représentent pas des données personnelles. Avec association de l'identité, les empreintes digitales sont au contraire des données sensibles, car elles peuvent déterminer l'appartenance raciale (ce qui n'est pas le cas des minuties). Dans ce dernier cas, une base de données est constituée et celle-ci est soumise aux dispositions de la loi fédérale sur la protection des données. Les données biométriques ne peuvent être traitées que sur la base d'un motif justificatif ou, si le maître du fichier est un organe fédéral, si une base légale le prévoit. Faute de motif justificatif, un tel traitement constitue une atteinte illicite à la personnalité, la personne concernée perdant, par l'action abusive d'un tiers, le contrôle sur ses propres empreintes digitales.

Le traitement de minuties associées à l'identité requiert la mise en place de mesures de sécurité adéquates, telles que le chiffrement des données impliquées. La protection doit s'étendre à tous les stades du traitement, y compris au stockage, à la comparaison et à la transmission des données personnelles. Le but du traitement des données doit être communiqué aux personnes concernées. En outre, l'employeur devrait consulter les employés avant d'introduire une telle mesure.

L'individualité et l'immuabilité des empreintes digitales ne permettent généralement pas une utilisation de celles-ci par des tiers. Par conséquent, les systèmes d'authentification biométrique réduisent fortement le risque de duplication, de vol, d'oubli ou de perte, comme cela peut être le cas avec les cartes ou badges de timbrage classiques. Ils représentent donc des moyens d'identification très efficaces, même si, dans de rares cas, les systèmes acceptent des photocopies d'empreintes digitales, des moulages de doigts ou des doigts morts. Le résultat de la comparaison des minuties étant basé sur des probabilités, une authentification erronée ne peut pas être exclue. Si les refus indus posent problème, les acceptations indues sont bien plus problématiques et nécessitent un contrôle complémentaire par le biais d'un numéro personnel d'authentification (PIN) ou d'un mot de passe. En outre, les empreintes digitales d'un doigt peuvent être altérées de manière provisoire ou durable, par exemple par un produit détergent ou une blessure. Pour cette raison, il est conseillé de recueillir des échantillons de référence de différents doigts de la même personne, afin de permettre l'authentification en cas d'altération d'une empreinte digitale. De plus, la reconstruction partielle ou complète d'une empreinte digitale à partir des minuties ne peut pas être complètement exclue. Bien que la perte de valeur probante des empreintes digitales suite à un abus représente un risque mineur, les spécialistes plaident incontestablement pour une utilisation très restrictive des empreintes digitales dans le domaine privé.

Dans le domaine privé et en particulier dans le domaine du travail, il est légitime de traiter des données personnelles à des fins de contrôle des présences. Dans certaines situations, ces données peuvent également servir au contrôle des mouvements à l'intérieur de l'entreprise (locaux avec accès limité et devant être sécurisés). Le recours à la biométrie garantit la fiabilité des données relatives aux présences des employés; en effet, la manipulation de ces données par l'employé n'est guère possible. Le risque qu'une base de données contenant des minuties d'empreintes digitales puisse être détournée de sa finalité est également très faible. En effet, on ne peut que très difficilement reconstituer l'image de l'empreinte digitale complète à partir des minuties. En outre, le risque de couplage de bases de données par des éléments biométriques est faible, car les algorithmes d'extraction des minuties ne sont à ce jour pas standardisés. D'ailleurs, un tel couplage serait relativement aisé à l'aide des éléments classiques de l'identité associés à ces données. Dès lors, la seule prévention contre des couplages qui permettraient d'établir des profils de personnalité réside dans la limitation des autorisations de couplage de ces bases de données.

En conclusion, si le stockage centralisé des empreintes digitales peut être problématique au niveau de la protection des données, le stockage centralisé des seules minuties (associées à l'identité) l'est bien moins, à condition toutefois que les mesures de sécurité prévues par la LPD soient appliquées. La prise d'empreinte, suivie de l'extraction des minuties, puis de la comparaison avec l'échantillon de référence présenté par l'employé (authentification), est manifestement la solution qui comporte le moins de risques pour la personnalité. En d'autres termes, le traitement de l'échantillon de référence dans une carte à puce à usage exclusif présentée par chaque employé lors du timbrage représente une solution plus proportionnée et donc compatible avec la législation sur la protection des données.

Au sujet de l'application de la biométrie dans le secteur privé, voir également chiffre 2.2.2.

7.3 Enregistrements sonores dans les salles de contrôle radar de Skyguide

Désireuse d'améliorer la sécurité aérienne, la compagnie Skyguide entend effectuer des enregistrements sonores intégraux dans les locaux de contrôle radar. Cette sauvegarde des moyens de preuve sonores a pour but de reconstituer précisément les circonstances entourant les accidents et les incidents graves. Du point de vue de la protection des données, l'introduction d'un tel système doit reposer sur une base légale (qui actuellement fait défaut) et doit respecter le principe de la proportionnalité. La nécessité d'une telle mesure doit en particulier encore être démontrée.

A la fin de l'année 2003, la société Skyguide SA et le délégué à la sécurité du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC) nous ont priés d'apprécier, à la lumière des principes de la protection des données, le projet consistant à enregistrer les conversations dans les locaux de contrôle radar de l'entreprise Skyguide par un système dénommé *Ambient Voice Recording Equipment (AVRE)*. Après avoir examiné la situation sur place, nous avons remis un rapport écrit à l'intention de Skyguide, de l'Office fédéral de l'aviation civile (OFAC), du Bureau d'enquête sur les accidents d'aviation (BEAA) et des syndicats des aiguilleurs du ciel.

Le système AVRE permettrait d'enregistrer toutes les conversations dans la salle de contrôle. Chacun des postes de travail devrait être muni d'un microphone permettant un enregistrement sonore intégral.

Selon les responsables, la sauvegarde intégrale des moyens de preuve sonores a pour but de permettre une reconstruction exacte des accidents ainsi que des incidents graves.

Selon le projet présenté – dans ses grandes lignes – par Skyguide, l'accès aux enregistrements se ferait à partir d'un système de code double (*dual code system*) et uniquement sur instruction du BEAA en cas d'accident ou d'incident grave. Skyguide possèderait la première partie du code d'accès, la seconde serait entre les mains des représentants du personnel; les deux parties seraient nécessaires pour accéder aux données. La transcription des enregistrements sur papier serait communiquée uniquement au BEAA et à l'OFAC.

Les informations traitées constituent des données personnelles au sens de la loi sur la protection des données, car elles peuvent être mises en relation avec des personnes identifiées ou identifiables. Selon les circonstances, les enregistrements peuvent contenir des données personnelles sensibles ou des profils de la personnalité.

Sous l'angle de la proportionnalité, la conservation intégrale des preuves sonores permise par le système AVRE est à même de faciliter la reconstitution d'accidents et d'incidents graves et permet d'améliorer la sécurité aérienne. Il n'est pas cependant pas tout à fait prouvé qu'un système de ce genre soit absolument nécessaire pour atteindre ces objectifs. En effet, ce ne serait pas seulement les enregistrements usuels téléphoniques ou radios entre les aiguilleurs du ciel et les pilotes dans le cockpit de l'avion qui seraient enregistrées. Le système AVRE ne permet pas du point de vue technique de différencier les entretiens professionnels des entretiens privés. D'ailleurs, selon l'Office fédéral de l'aviation civile, aucun autre pays n'a jusqu'ici introduit un système d'enregistrement aussi complet et ce système n'est recommandé par aucune organisation internationale de l'aviation civile. Cependant on peut reconnaître que le système AVRE est apte à reconstruire les responsabilités personnelles au sein même de l'entreprise Skyguide

Toujours selon le principe de la proportionnalité, il convient d'avoir un rapport raisonnable entre le but du traitement et l'atteinte à la personnalité. D'un côté, il est clair qu'il existe un intérêt légitime à la reconstitution facilitée des accidents ou des incidents graves, à la détermination des responsabilités personnelles et à une amélioration de la sécurité aérienne. D'un autre côté, le seul fait de savoir qu'on est enregistré est à même de susciter des sentiments négatifs qui, outre une détérioration de l'ambiance de travail, sont aussi susceptibles de provoquer une pression psychique et des répercussions physiques non négligeables. Dans ce cas, l'atteinte à la personnalité serait considérable et ne toucherait pas seulement les personnes responsables d'un accident ou d'un incident grave, mais tous les employés du contrôle aérien. La détérioration des prestations de service des employés ainsi que l'augmentation de l'absentéisme en raison d'un besoin croissant de plages de temps non surveillées pourraient figurer parmi les répercussions négatives du système AVRE.

Toutefois, si l'on informe préalablement les employés sur le fait que les enregistrements sont en principe inaccessibles et sur le système de double code en cas d'exploitation concrète des données, on peut réduire considérablement l'impression de surveillance constante et, par-là l'atteinte à la personnalité. De plus, il conviendra également d'informer les employés avec précision sur les finalités du système AVRE, sur l'objet et l'étendue des enregistrements, la procédure d'exploitation, la durée de conservation et le droit d'accès.

Dans tous les cas, les enregistrements ne devront être exploités qu'en cas d'accident ou d'incident grave et uniquement sur injonction du Bureau d'enquête sur les accidents d'aviation. En d'autres termes, les enregistrements obtenus par le système AVRE ne doivent être accessibles que si certaines conditions, cumulatives et restrictives, sont remplies.

En l'absence de projet concret, il ne nous est cependant pas possible actuellement d'apprécier le caractère proportionné du système AVRE. La question de la nécessité de cette mesure est en particulier laissée ouverte. Dans ces circonstances, nous avons recommandé à Skyguide d'examiner et de prendre des mesures moins attentatoires à la personnalité des personnes concernées.

En outre, même si la mesure devait s'avérer nécessaire sous l'angle du principe de la proportionnalité, il conviendrait d'introduire une base légale. Les personnes physiques ou morales qui, comme Skyguide, se voient attribuer des tâches publiques de la Confédération ont en effet besoin d'une base légale pour tout traitement de données. Pour le système AVRE, il est donc nécessaire de disposer d'une réglementation précise concernant en particulier la ou les finalités du traitement de données, l'organisation du système, les autorisations d'accès, les catégories de données enregistrées, la procédure d'exploitation, le ou les responsables du fichier et le cercle des personnes concernées. Or il n'existe actuellement pour un tel système de traitement des données ni réglementation nationale, ni normes internationales.

8 Economie et commerce

8.1 Exigences générales pour le traitement des données relatives aux véhicules à moteur

Les véhicules à moteur sont de plus en plus nombreux à être équipés de technologies modernes (GPS, puces) ayant en mémoire des informations sur les itinéraires et les habitudes de conduite. On peut à ce propos émettre des réserves du point de vue de la protection des données. Il convient en premier lieu de déterminer s'il s'agit en l'occurrence de données personnelles. Dans l'affirmative, la question se pose de savoir quelles données sont sauvegardées, quelle est l'étendue et la finalité du traitement. Enfin, il est également important de savoir comment les données sauvegardées sont protégées contre un accès non autorisé.

Selon la définition de l'art. 3 de la loi sur la protection des données (LPD), toutes les informations qui se rapportent à une personne identifiée ou identifiable sont des données personnelles. Une personne est identifiable lorsque l'on peut lui attribuer une information sans mettre en œuvre des moyens excessifs. Etant donné que le détenteur- en règle générale aussi le conducteur- d'un véhicule immatriculé est de toute manière identifiable, les informations concernant le véhicule doivent être en principe considérées comme des données personnelles. Pour ce qui est des données relatives au moteur et à l'exploitation d'un véhicule, il convient de faire la distinction entre les informations qui se rapportent aux habitudes de conduite ou qui permettent de tirer des conclusions à ce propos (par ex. les données concernant la vitesse, le nombre de tours, la manière de passer les vitesses) et les informations qui ne concernent que l'état technique du véhicule (niveau d'huile, pression des pneus, etc.). Dans le dernier cas, il ne semble pas y avoir de rapport suffisamment étroit avec une personne déterminée. Par contre, les enregistrements de données géographiques de navigation (par ex. les coordonnées GPS) doivent être considérées comme des données personnelles.

La LDP est applicable lorsque les données relatives au moteur et l'exploitation du véhicule sont considérées comme des données personnelles. Dans ce cas, la collecte et le traitement réguliers de ces données ne sont permis que s'ils sont licites et les principes fondamentaux de la protection des données doivent être respectés.

Tout traitement de données doit reposer sur un *motif justificatif*. Dans le présent contexte, le consentement des personnes concernées ou l'exécution du contrat peuvent servir de motif justificatif. Mais indépendamment de cela, le contrat doit indiquer de

manière suffisamment précise les traitements prévus, comme l'exige le *principe de transparence*. Il convient en conséquence d'informer le détenteur du véhicule du but dans lequel les données sont enregistrées, de quelles données il s'agit, du lieu où elles sont enregistrées ou rendues accessibles et par qui, et enfin de l'analyse des données qui sera faite.

Sous l'angle de la protection des données, les traitements de données qui sont effectués dans le cadre de travaux d'entretien ou de réparation à des fins de prestation de garantie ou de service ne posent pas de problèmes. Mais si le traitement va plus loin (si par exemple plus de données que nécessaire sont traitées ou qu'elles le sont dans un autre but que celui indiqué) il n'est licite que si les personnes concernées en sont informées et ont donné leur consentement. Dans toute la mesure du possible, les données doivent être traitées après avoir été rendues anonymes, conformément au principe de proportionnalité.

Les personnes procédant au traitement sont en outre tenues de garantir *la sécurité des données* en prenant des mesures techniques et organisationnelles appropriées. Citons par exemple le contrôle des utilisateurs et des accès, ainsi que le cryptage des données.

Il convient de tenir compte des exigences légales que doit remplir une transmission à l'étranger des données relatives au moteur et à l'exploitation. Rappelons à cet égard que les exigences en matière de protection des données en vigueur dans les pays de l'UE sont en général similaires à celles en vigueur en Suisse.

Si l'analyse de données relatives au moteur, à l'exploitation ou encore de données géographiques de navigation concerne une voiture de service ou d'entreprise, il convient de veiller aussi, selon les circonstances, au respect des exigences légales relatives à la surveillance des collaborateurs à leur poste de travail. Cela pourrait par exemple être le cas lorsque l'exploitation de ces données concerne certains collaborateurs qui ont besoin de ce véhicule pour accomplir une part essentielle de leur activité (par ex. les collaborateurs des services extérieurs); ce genre de surveillance n'est licite qu'exceptionnellement et dans certaines conditions.

La police et les autorités de poursuite pénale peuvent, dans le cadre des bases légales applicables – consulter les données relatives au moteur et à l'exploitation du véhicule. Par contre, si une assurance responsabilité civile entend utiliser les données concernant le moteur et l'exploitation du véhicule, elle doit pouvoir se fonder sur le consentement de la personne lésée ou sur un intérêt public ou privé prépondérant.

De plus en plus, des données déjà collectées sont utilisées dans des buts non déclarés, par exemple dans le cadre de campagnes de marketing. Pour cette raison également, il convient de ne pas enregistrer de données si cela n'est pas absolument nécessaire ou d'effacer périodiquement les données enregistrées. Du point de vue de la protection des données, cela correspond également au principe de la proportionnalité dont on déduit, entre autres, la règle voulant que l'on évite la collecte de données et que l'on diminue leur utilisation (Prinzip der Datenvermeidung und -sparsamkeit). Pour les mêmes raisons, le traitement doit avoir lieu, si possible, sous une forme anonyme ou au moins pseudonymisée. L'établissement du diagnostic au garage ou chez le fabricant peut sans problème être fait sous forme pseudonymisée et le détenteur du véhicule est seulement identifié lorsque cela est vraiment indispensable, par exemple dans le cadre de prestations de garantie.

En principe, il est important que les clients soient clairement informés des données relatives à l'exploitation et au véhicule qui sont enregistrées dans le véhicule, quelles sont les données qui sont rendues accessibles à des fins d'entretien, par qui (garagiste, fabricant, tiers) et quels sont les traitements supplémentaires qui sont entrepris (par ex. à des fins de marketing). En effet, ce n'est qu'ainsi que les clients ont la possibilité de décider quels traitement ils acceptent.

8.2 Transmission et utilisation de données-clients par un importateur d'automobiles

Un garagiste doit-il transmettre à son importateur les données-clients qu'il a obtenues à partir d'un contrat de vente? Le garagiste concerné peut ne pas apprécier que l'importateur écrive directement à ses clients pour leur proposer de s'adresser à un autre garage assurant désormais la représentation de la marque. Il est néanmoins admis que l'importateur utilise des données-clients si certaines conditions sont remplies.

Un importateur d'automobiles a réorganisé son réseau de concessionnaires. Dans ce contexte, il a écrit aux propriétaires de véhicules de cette marque pour leur faire savoir que la concession avait été retirée à leur garagiste qui la possédait jusqu'ici. Par ailleurs, il a proposé à ces personnes de s'adresser à un nouveau concessionnaire. Dans la même lettre, l'importateur de voitures précisait que les propriétaires de véhicules avaient la possibilité de s'opposer au transfert de leurs données-clients vers le nouveau représentant de la marque. De nombreux garagistes à qui la concession avait été retirée ont estimé que les démarches de l'importateur d'automobiles violaient la loi fédérale sur la protection des données.

Nous avons procédé à un examen des faits et avons constaté ce qui suit:

C'est avec l'accord des propriétaires des véhicules concernés que le garagiste (qui possédait la concession jusque-là) a transmis les données-clients à l'importateur, à des fins de marketing.

Selon la loi sur la protection des données, tout traitement de données – dans le cas d'espèce la transmission de données-clients – nécessite un motif justificatif. Le consentement de la personne concernée constitue un motif justificatif. Le consentement peut être donné explicitement ou tacitement. Les exigences en matière de consentement dépendent en particulier du caractère sensible des données personnelles traitées. En l'occurrence, les clients avaient été informés dans les conditions générales accompagnant le contrat de vente que leurs données seraient communiquées à l'importateur. Le garagiste a donc transmis ses propres données-clients conformément aux principes de la protection des données.

L'importateur d'automobiles a informé les propriétaires de véhicules qu'il prévoyait de communiquer leurs données-clients et que le but du traitement de ces données allait de ce fait être modifié. Les propriétaires de véhicules avaient la possibilité de s'opposer au transfert de ses données au nouveau concessionnaire.

Le transfert des données-clients par l'importateur constitue une modification du but initial du traitement. L'importateur d'automobiles a informé par écrit les clients du fait qu'il entendait transférer leurs données. Il leur a donné la possibilité de s'y opposer dans un délai déterminé. Les données-clients en question ne sont pas des données personnelles sensibles. Le consentement exprès des clients au transfert de leurs données n'était de ce fait pas nécessaire. L'absence de réaction du client peut donc être considérée comme consentement valable au sens de la loi sur la protection des données.

Par ailleurs, s'agissant du traitement des données-clients, l'importateur peut invoquer que le traitement est en relation directe avec la conclusion ou l'exécution du contrat (intérêt privé prépondérant). Il peut contacter directement les clients pour leur communiquer qu'il entend modifier son réseau de concessionnaires. Cela vaut notamment lorsque ces modifications ont des répercussions sur le rapport contractuel entre le garagiste, à qui la concession doit être retirée, et ses clients (si par exemple le contrat prévoit des prestations de garantie que seul un concessionnaire de la marque peut remplir). Mais l'importateur ne peut pas, sans le consentement des clients, transmettre les données personnelles des clients à d'autres garagistes qui ont désormais la représentation de la marque.

La loi sur la protection des données n'accorde au précédent garagiste aucun droit sur les donnés-clients qu'il a communiquées à l'importateur conformément aux dispositions de protection des données (c'est-à-dire avec l'accord préalable des personnes concernées)

Conformément à la loi sur la protection des données, seules les personnes dont les données sont traitées ont le droit de s'opposer au traitement de ces données. Les participants à un fichier, en l'occurrence les garagistes, ne peuvent faire valoir aucun droit quant au traitement des données par eux collectées et transmises à des tiers.

Compte tenu de ce qu'il précède, nous sommes arrivés à la conclusion que la transmission des données-clients par l'importateur était conforme à la loi sur la protection des données.

9 International

9.1 Conseil de l'Europe

9.1.1 Travaux du T-PD: données biométriques – droits des personnes concernées – Internet

Le Comité consultatif de la Convention 108 (T-PD) et son bureau ont axé leurs travaux sur l'élaboration d'un rapport sur l'application des principes de la convention 108 à la collecte et au traitement de données biométriques, à l'examen de la pertinence des principes de base de la protection des données aux réseaux mondiaux de télécommunication et à l'analyse des droits et responsabilités des personnes concernées.

Suite à la restructuration intervenue au Conseil de l'Europe et notamment à la suppression du Groupe de projet sur la protection des données (CJPD) (voir notre 11ème rapport d'activités 2003/2004, chiffre 11.1.2), le T-PD demeure le seul comité au sein du Conseil de l'Europe en charge des questions de la protection des données. Le comité est composé de représentants de l'ensemble des Etats ayant ratifié la Convention 108. Les autres pays membres du Conseil de l'Europe peuvent participer aux travaux en tant qu'observateurs. Le comité a mis en place un bureau chargé de préparer les travaux du comité. Ce bureau est composé de 7 représentants des Etats parties, dont le représentant au titre de la Suisse.

Le travail du comité s'est axé en priorité sur l'élaboration d'un rapport sur l'application des principes de la Convention 108 à la collecte et au traitement de données biométriques. Ce rapport a été adopté par le comité lors de sa 20ème réunion plénière du 2 au 4 février 2005. Il est conçu comme un rapport d'étape. Le comité n'a pas souhaité élaborer un instrument juridique régissant un domaine en pleine évolution. Il a préféré donner des orientations basées sur l'état des connaissances actuelles. Le comité envisage d'élaborer un instrument juridique dans une étape ultérieure, si nécessaire. Dans ses conclusions, il a néanmoins convenu que lors du recours à des données biométriques, les principes suivants devraient en particulier être pris en considération

- évaluation des avantages et des inconvénients du recours à la biométrie pour la vie privée des personnes concernées, prise en compte des solutions alternatives et choix du système qui interfère le moins avec la vie privée;
- respect du principe de finalité;

- respect du principe de proportionnalité: en particulier, un système de traitement des données ne devrait pas permettre de collecter et de traiter plus de données personnelles que sa finalité ne l'exige;
- il faut éviter de recourir à des solutions d'identification des personnes concernées lorsqu'une opération de vérification est suffisante pour la finalité du traitement ;
- en cas de vérification de l'identité des individus, les données biométriques devraient être stockées de préférence sur un support individuel sécurisé de stockage (par ex. une carte à puce);
- information des personnes concernées sur la finalité du système, l'identité du responsable de traitement, les données traitées et les catégories de destinataires;
- respect du droit d'accès et de rectification;
- respect du principe de sécurité des données;
- développement de procédure de certification et de contrôle;
- existence de procédure de réexamen en cas de rejet d'une personne enrôlée dans un système biométrique.

Le comité a en outre débuté l'examen de la pertinence des principes de la Convention 108 aux réseaux mondiaux de télécommunications et notamment de l'Internet. Il a en particulier pris connaissance d'un rapport d'experts. Ce rapport parvient à la conclusion que les principes de la Convention 108 répondent au défi actuel de l'Internet et des nouvelles technologies. Toutefois, le rapport suggère de compléter la Convention par de nouveaux principes destinés à favoriser l'autodétermination informationnelle dans l'environnement technologique actuel et notamment les principes du chiffrement et de l'anonymat «réversible», de la réciprocité des avantages, de la promotion de solutions technologiques conformes au respect des exigences de protection des données ou améliorant la situation des personnes protégées par le droit, de la maîtrise par l'utilisateur du fonctionnement des équipements terminaux et de l'octroi des moyens de protection des consommateurs, à l'utilisateur de certains systèmes d'information. Le comité a chargé son bureau de procéder à une analyse plus approfondie de ce rapport afin de déterminer quelles actions devraient être entreprises dans le futur.

Suite à une conférence consacrée aux droits et responsabilités des personnes concernées par les données, organisée conjointement par le Conseil de l'Europe et le Bureau pour la protection des données de la République Tchèque à Prague du 14 au 15 octobre 2005, le comité consultatif a décidé de renforcer la sensibilisation des personnes concernées et des responsables de traitement (voir ci-dessous, chiffre 9.1.2). Dans ce cadre, le comité consultatif a accepté la proposition suisse d'instaurer une

journée européenne de la protection des données. Cette journée aurait lieu chaque année en date du 28 janvier. Il revient au Comité des Ministres du Conseil de l'Europe de donner le feu vert à cette initiative. Enfin, le comité consultatif a également convenu de donner suite à notre proposition d'ancrer dans les instruments du Conseil de l'Europe le droit fondamental à la protection des données.

9.1.2 Conférence sur les droits et les responsabilités des personnes concernées par les données

Du 14 au 15 octobre 2004 s'est tenue à Prague une conférence sur les droits et les responsabilités des personnes concernées par les données, organisée par le Conseil de l'Europe et le Bureau pour la protection des données de la République Tchèque. Cette conférence a mis l'accent sur la nécessité de renforcer la sensibilisation des individus quant à leurs droits et leurs responsabilités en matière de protection des données.

La conférence avait pour thèmes principaux la sensibilisation des personnes concernées par les données sur leurs droits et responsabilités afin d'en faire des acteurs de leur propre protection, l'information des personnes concernées, le consentement et la mise en œuvre des droits. Les participants se sont en particulier interrogés sur la manière d'améliorer les connaissances des individus en matière de protection des données. En effet, la globalisation des technologies de l'information et de la communication (systèmes d'information sans frontières aux capacités de traitement illimités) a notamment pour conséquence de diminuer singulièrement la maîtrise des individus sur leurs propres informations. Ceux-ci ont une connaissance insuffisante des droits que leur confèrent les législations de protection des données. Les responsables de traitement sont quant à eux peu enclins à respecter lesdites législations. Ainsi, il paraît nécessaire de compléter les législations par l'autoréglementation, par des procédures de certification et par des solutions technologiques. La sensibilisation ne doit pas être le seul fait des autorités. Il faut recourir à d'autres acteurs, notamment les fournisseurs de service, les producteurs d'équipement et des organisations de défense des droits des individus. Une plus grande transparence est nécessaire pour les traitements de données personnelles et les individus doivent êtres orientés sur le fonctionnement des systèmes d'informations, notamment afin de permettre à chacun de mieux comprendre son propre environnement informationnel. Cela est d'autant plus important qu'aujourd'hui la grande part de nos actions et de l'utilisation de moyens technologiques débouchent sur des traitements de données personnelles. Les autorités de protection des données doivent intensifier leur action d'information et d'éducation des personnes concernées et des responsables de traitement. Ils doivent assurer une

meilleure écoute des citoyens et notamment leur offrir une information conviviale. Enfin, les autorités doivent intensifier leurs activités de contrôle, ce qui suppose qu'on leur accorde les moyens et ressources nécessaires. La sensibilisation passe également par l'éducation et l'intégration de la protection des données dans les programmes scolaires et universitaires, ainsi que la mise en place de formations en protection des données.

9.2 Union européenne

9.2.1 La protection des données et les Bilatérales II

La mise en œuvre des accords bilatéraux entre la Suisse et l'Union européenne (Bilatérales II) implique la nécessité d'adapter divers textes de loi suisses. Les dispositions relevant du droit de la protection des données sont également concernées. En effet, la protection des données revêt une importance particulière dans les deux accords d'association à Schengen/Dublin.

Dans le cadre des accords associant la Suisse à Schengen et à Dublin, tout traitement de données personnelles effectué dans les domaines relevant du premier pilier de l'Union européenne (à savoir contrôles aux frontières, visas, armes à feu, stupéfiants et asile) doit respecter les exigences posées par la directive 95/46/CE sur la protection des données dans l'UE. La transposition du contenu matériel de cette disposition nécessite la révision des lois spéciales suisses y relatives.

L'application des Accords bilatéraux II implique d'introduire dans les lois fédérales sur le séjour et l'établissement des étrangers, sur l'asile et sur les armes une disposition identique; celle-ci règle les possibilités de communication de données d'une autorité suisse aux Etats ne faisant pas partie de Schengen. Selon la directive de l'UE sur la protection des données, une telle transmission de données n'est admise que si l'Etat tiers garantit un niveau de protection des données adéquat. Dans le cas contraire, la communication de données peut quand même se faire sous certaines conditions, notamment si le destinataire des données présente, dans le cas d'espèce, des garanties suffisantes pour la protection de la personnalité de la personne concernée. A cet égard, le Conseil fédéral sera chargé de régler l'étendue des garanties à fournir et leurs modalités. Dans le cadre de la procédure de consultation du message sur les Accords bilatéraux II, nous avons demandé que le Préposé fédéral à la protection des données soit chargé de cette fonction. En effet, l'autorisation de communiquer des données n'est pas une appréciation d'ordre politique, mais relève uniquement de la

protection des données. Le Préposé fédéral à la protection des données dispose des connaissances nécessaires pour déterminer quelles garanties doivent être prises pour la protection de la personnalité des personnes concernées et est ainsi mieux à même que le Conseil fédéral à remplir cette fonction.

S'agissant de la protection des données dans les domaines de Schengen relevant du troisième pilier de l'UE (coopération policière et judiciaire en matière pénale) et dans lesquels la directive sur la protection des données n'est donc pas applicable, la convention d'application de l'accord de Schengen contient des dispositions spécifiques de protection des données qui sont en grande partie directement applicables (ce qui signifie que les autorités suisses doivent appliquer directement sans transposition de l'accord dans le droit suisse). Au cas où une transposition dans le droit suisse devait s'avérer nécessaire, la base légale formelle requise sera créée dans le code pénal.

Dans le cadre de Schengen/Dublin, le Préposé fédéral à la protection des données devra assumer des fonctions supplémentaires (autorité de contrôle nationale en matière de protection des données dans le cadre du Système d'information de Schengen (SIS), participation en tant que membre à part entière aux travaux de l'autorité de contrôle commune, participation au groupe de protection des personnes à l'égard du traitement de données personnelles prévu par l'art. 29 de la directive sur la protection des données 95/46/CE, au comité au sens de l'art. 31 de la même directive et enfin au groupe de travail protection des données dans le domaine relevant du troisième pilier). Le Préposé fédéral à la protection des données ne pourra assumer ces nouvelles tâches que s'il dispose de ressources supplémentaires. En outre, cet élargissement des tâches implique des coûts supplémentaires qui devront être pris en compte dans le budget du PFPD.

9.2.2 Conférence européenne des commissaires à la protection des données

La Conférence européenne des commissaires à la protection des données s'est réunie à Rotterdam du 21 au 23 avril 2004 et à Wroclaw le 14 septembre 2004. Elle a en particulier adopté les règles d'accréditation des autorités de protection des données auprès de la conférence.

La conférence a réuni les commissaires à la protection des données de 31 Etats européens ayant ratifié la Convention 108, dont les 25 Etats membres de l'Union européenne. La Bosnie- Herzégovine assistait à la conférence à titre d'observateur. Les délégués des autorités de contrôle des Commissions européennes, d'Europol, Schengen et Eurojust, ainsi que des représentants de la Commission européenne et du Secrétariat du Conseil de l'Europe ont assisté aux travaux.

La première session de la conférence était consacrée à l'analyse du rôle des autorités de protection des données. Selon le rapporteur, Prof. Colin J. Bennett de l'Université de Victoria (Canada), la globalisation de la société a également eu des conséquences sur le rôle, l'organisation et l'approche des autorités de protection des données. La mise en œuvre des principes de la protection des données est différente d'un Etat à l'autre et plusieurs instruments se côtoient: modèle d'autorisation, commissaire à la protection des données, modèle d'enregistrement, auto-contrôle. Le rôle des autorités de protection des données évolue et celles-ci concilient différentes casquettes: médiateur, contrôleur, conseiller, éducateur, formateur, négociateur, avocat, ambassadeur, etc.). La recherche de solutions concertées avec les différents acteurs est de plus en plus privilégiée. Acteurs indispensables des instruments de la protection des données, les autorités de protection des données doivent renforcer leur présence et leur collaboration, et prendre conscience qu'elles constituent une force. Il serait souhaitable qu'elles adoptent plus souvent des résolutions au niveau international. En outre, le rôle proactif et général doit être plus important que le rôle réactif et spécifique.

Lors de la deuxième session, la conférence s'est interrogée sur la politique de communication et sur l'interaction des autorités de protection des données avec le monde extérieur. La Commission européenne a présenté le résultat d'une vaste enquête effectuée dans tous les Etats membres de l'UE auprès des responsables de traitement et auprès des citoyens. Il ressort de ces enquêtes qu'il est nécessaire de renforcer les ressources pour la sensibilisation et l'information du public. Les commissaires sont conscients de l'existence de lacunes dans l'information. Ils estiment nécessaires de mettre l'accent sur la sensibilisation, la formation, l'information et les politiques de communication.

La troisième session a abordé les questions de mise en œuvre. Après avoir entendu des exposés sur certains systèmes nationaux, les commissaires en ont appelé à une meilleure harmonisation des mécanismes opérationnels et notamment au développement d'actions conjointes. Ils ont relevé l'importance des échanges d'information.

La quatrième session était consacrée à l'organisation interne des autorités de protection des données et notamment à la manière d'améliorer leur efficacité et leur image à l'extérieur. Les commissaires sont d'avis qu'il est fondamental de veiller aux intérêts des citoyens et d'œuvrer à l'acceptation de la protection des données dans la société.

Lors de la cinquième session, les commissaires ont abordé des questions liées à la coopération judiciaire dans l'Union européenne. Ils ont rappelé l'importance de la protection des données et la nécessité d'avoir des règles communes. On a relevé certains problèmes liés au cadre juridique, aux différentes instances impliquées (organisations internationales (Europol, Schengen, Interpol, Conseil de l'Europe) et nationales) et aux approches différentes. En particulier, plusieurs Etats ont conclu des accords bilatéraux dans lesquels la protection des données est traitée de manière diverse, avec le risque d'affaiblir le cadre en place. Or, il est nécessaire d'avoir une approche globalisée et pragmatique de la protection des données.

Les commissaires sont d'avis que les autorités de protection des données d'Europol, Schengen, Eurodac, Eurojust et des commissions européennes devraient à terme être réunies en une seule autorité. Cela nécessitera des changements institutionnels. Dans cette optique, ils ont créé un groupe de travail de la conférence qui sera chargé de définir une stratégie et des objectifs à atteindre et qui devra en particulier se pencher sur les mesures de lutte contre le terrorisme préconisées par l'UE.

La Conférence a adopté une directive fixant ses critères d'admission. Elle entérine ainsi l'élargissement de la Conférence à l'ensemble des Etats européens ayant ratifié la Convention 108 conformément aux propositions que nous avions faites lors de la Conférence de Séville en 2003. La Conférence a mis en place un comité d'accréditation composée de l'Espagne, des Pays-Bas et de la Pologne.

9.3 OCDE

9.3.1 Groupe de travail sur la sécurité de l'information et la protection de la sphère privée (WPISP)

Au cours de l'année écoulée, le groupe de travail a examiné l'application des nouvelles directives de l'OCDE concernant la sécurité de l'information ainsi que la création d'un site Internet et d'un outil de formation en ligne consacré à la sécurité. Il a également abordé d'autres thèmes, à savoir le renforcement des mesures augmentant la sécurité du trafic voyageurs au niveau international, l'état de la mise en oeuvre des procédures d'identification dans les Etats membres et les exigences en matière de transparence dans les déclarations de protection des données.

Le groupe de travail a élaboré un questionnaire qui a permis de relever, auprès des Etats membres, un certain nombre de données concernant l'application des directives en matière de sécurité. Cette enquête avait pour but de définir les domaines sur lesquels il convient encore de concentrer les efforts. Parallèlement au questionnaire, un inventaire répertoriant les différentes méthodes de sécurité appliquées dans les Etats membres a été établi.

Par ailleurs, le secrétariat a créé un site Internet consacré à la sécurité. Ce site permet d'obtenir en tout temps une vue d'ensemble complète sur les méthodes de sécurité appliquées par les Etats membres.

Le groupe de travail a décidé de développer un outil de formation en ligne afin de faciliter l'application des mesures de sécurité par les PME et les utilisateurs finaux. Cet instrument indiquera les différentes possibilités en matière de sécurité et contribuera à sensibiliser davantage les entrepreneurs et les utilisateurs. Le groupe de travail disposant de ressources limitées, la question s'est posée de savoir si l'OCDE devrait créer son propre outil ou devrait plutôt développer la mise au point d'un outil déjà existant. L'élaboration d'un outil de sécurité uniforme satisfaisant à toutes les exigences nationales et internationales serait très difficile à réaliser en raison des différences au niveau des systèmes d'exploitation et des structures d'entreprises. Il serait donc préférable d'envisager des outils en ligne permettant diverses analyses de sécurité sur la base de listes de contrôle (check-lists); celles-ci devraient se présenter sous une forme simple pour que les PME puissent aussi les utiliser. Il convient néanmoins de relever qu'il sera difficile de mettre au point de telles listes de contrôle utilisables par les PME du monde entier. On pourrait donc envisager de reprendre une norme de sécurité internationale (par ex. ISO 17799) afin de contrôler par ce canal le premier

niveau de sécurité. En même temps, les exigences spécifiques aux pays pourraient y être intégrées (comme dans le générateur de déclaration de politique de la vie privée de l'OCDE). Le secrétariat élaborera une solution en collaboration avec quelques pays membres et la présentera au cours de la prochaine séance.

Comme autre thème, le groupe de travail a traité de la sécurité en matière de circulation des voyageurs à l'échelle internationale. L'OCDE s'est fixé comme but de renforcer les vérifications de l'identité des voyageurs. A cet effet, il convient de veiller à ce que les différentes solutions techniques puissent fonctionner en synergie (interopérabilité). Toutefois, la circulation des voyageurs ne devrait pas s'en trouver entravée inutilement. De plus, la garantie d'un trafic voyageurs sûr et efficace ne doit pas se faire aux dépens de la sphère privée des passagers. C'est pourquoi, en plus de la participation du groupe de travail ad hoc de l'OACI, les travaux du Conseil de l'Europe et du groupe de travail de l'UE prévu par l'art. 29 de la Directive sur la protection des données (95/46/CE) seront également pris en compte; en effet, ces deux organes ont déjà pour domaines d'activités la biométrie et la sécurité en matière de trafic voyageurs. Le groupe d'experts a commencé d'examiner les principes régissant l'utilisation des caractéristiques biométriques permettant de vérifier l'identité des voyageurs. Des informations pratiques sont recueillies à cet effet afin d'établir une ligne de conduite prenant en compte les exigences de la protection et de la sécurité des données. Dans une première phase des travaux, il est prévu d'élaborer une banque de données des passeports volés et perdus.

Les Etats-Unis ont clairement montré leur intérêt pour les banques de données biométriques, notamment celles permettant un échange constant de données (*cross-border realtime information sharing*). A cet égard ils ont trois priorités: la protection et la sécurité des données, l'échange de données au niveau mondial et l'examen des solutions techniques. En parallèle, les autorités américaines ont déclaré de manière claire et sans équivoque qu'il convenait d'accélérer les travaux dans ce domaine.

Un rapport du Conseil de l'Europe en matière de biométrie a été également présenté. Dans ce domaine sensible, très complexe du point de vue technique, les principes fondamentaux sur la biométrie n'ont pas été abordés d'emblée, contrairement à ce qui se fait d'ordinaire. Il s'agit en fait d'un rapport d'étapes. Il traite des questions de sécurité (notamment la sécurité de l'accès aux données), de la finalité et de l'utilisation des données, de la vérification de leur authenticité et de la sauvegarde par des tiers. Le rapport final présentera un bilan en matière de biométrie, dans lequel il indiquera les risques, les exigences en matière de sécurité et la nécessité de l'interopérabilité et traitera des questions de sauvegarde centrale et décentralisée.

Dans le domaine de l'authentification électronique, un questionnaire circule actuellement dans tous les Etats membres. Celui-ci a pour but de déterminer à quel stade en est l'application des procédures d'authentification, dont font partie toutes les technologies appliquées dans ce contexte, ainsi que les barrières (techniques en particulier) qui entravent la suite des travaux.

Le groupe de réflexion constitué par l'OCDE pour aborder le problème des messages publicitaires indésirables (*spams*) s'est donné comme but de créer un outil anti-spams complet qui doit servir d'instrument de formation et d'information pour les utilisateurs. Ce groupe travaille également à la concrétisation des exigences légales et à la mise à disposition de variantes techniques.

Enfin, le groupe de travail a examiné les exigences en matière d'information et de transparence dans le traitement des données personnelles (appelées également «déclarations de protection de la vie privée», en anglais «*privacy notices*» ou encore «*global multi-layered notices*»). La résolution relative aux déclarations de protection de la vie privée adoptée lors de la 25ème Conférence internationale de Sydney sur la protection des données a été analysée. En outre, il a été constaté que les déclarations de protection de la vie privée sont actuellement, et d'une manière générale, non seulement trop longues, mais aussi difficilement compréhensibles pour les utilisateurs. Les autorités de protection des données tout comme le secteur privé sont unanimes à penser que ces déclarations doivent être simples, brèves et claires. Par ailleurs, les déclarations de protection de la vie privée d'un site Internet doivent être faciles à trouver. Pour plus de détails sur les exigences auxquelles les déclarations de protection de la vie privée doivent répondre, voir aussi notre 6ème rapport d'activités 1998/99, chiffre 4.1. Relevons par ailleurs dans ce domaine la récente proposition de l'organisation nord-américaine e-trust de mettre à disposition un format mondial uniforme (*common template*) afin d'améliorer, pour les utilisateurs, la compréhensibilité des déclarations. Les différentes organisations adeptes d'un format uniforme reconnu au niveau international et d'une déclaration de protection de la vie privée brève, mais informative, approuvent ce procédé tout comme le groupe UE de l'art. 29.

Le secrétariat a proposé de ne pas lancer de nouveaux travaux sur les déclarations de protection de la vie privée, mais de suivre les travaux déjà en cours et cas échéant d'y participer. L'OCDE s'est fixé comme but d'élaborer un modèle de déclaration pouvant être produit automatiquement par le générateur de déclaration de politique de la vie privée de l'OCDE.

Ce modèle de déclaration n'a pas pour but de présenter une solution globale, compatible avec toutes les dispositions nationales, mais de fournir une déclaration de protection de la vie privée uniforme (format et texte) dont la précision permettra à l'utilisateur de distinguer nettement les différences dans les traitements de données personnelles effectuées par des entreprises d'une même branche ou d'un autre pays.

Toutes les délégations ont salué les travaux visant une amélioration des déclarations de protection de la vie privée, notamment parce qu'elles permettent non seulement de mieux satisfaire aux exigences légales en matière de transparence, mais parce qu'elles offrent aux utilisateurs finaux une utilité pratique et immédiate.

9.4 Autres thèmes

9.4.1 Conférence internationale des commissaires à la protection des données

La 26ème Conférence internationale des commissaires à la protection des données s'est tenue à Wroclaw du 14 au 16 septembre 2004. Elle réunissait des délégations provenant d'une quarantaine d'Etats du monde entier. La conférence avait pour thème général «Droit à la vie privée – Droit à la dignité». Les commissaires ont adopté une résolution sur le projet de normes ISO de protection de la vie privée.

La 26ème Conférence internationale des commissaires à la protection des données, qui avait pour thème «Droit à la vie privée – Droit à la dignité», s'est déroulée à l'Université de Wroclaw à l'invitation de l'autorité polonaise de la protection des données. La Pologne est le premier pays d'Europe centrale à accueillir la conférence internationale. Le choix du thème de la conférence et de la ville hôte, carrefour entre diverses nations et cultures marquées par l'histoire, ont contribué à rappeler à quel point le traitement des données personnelles pouvait, en l'absence de contrôle démocratique, déboucher sur la négation de la dignité humaine.

La conférence a souligné l'importance des instruments, notamment juridiques, de protection des données pour garantir le respect de la dignité humaine. Comme à l'accoutumée, la conférence a permis un large échange d'idées et d'expériences entre les commissaires à la protection des données, les représentants des organisations internationales, de l'économie, des médias et du monde académique et scientifique. Elle a permis non seulement d'évaluer les risques d'atteinte aux libertés et aux droits fondamentaux, notamment en raison des développements technologiques et de

l'universalité de l'information, mais aussi d'aborder les moyens de protéger la vie privée. Les thèmes ont été discutés dans le cadre de séances plénières et des sessions parallèles. La conférence a en particulier débattu du droit à la vie privée et de la protection de la sécurité publique, des technologies de la radio-identification (RFID), de la protection de la vie privée dans le domaine de l'emploi, du droit à la vie privée face aux médias, de l'e-démocratie et des flux transfrontières de données. Elle a permis de confronter les autorités de protection des données aux attentes de l'économie et notamment de constater que la protection des données a un coût parfois élevé, mais qui se révèle un atout bénéfique pour les entreprises. Elle a mis l'accent sur la collaboration internationale, notamment entre autorités de protection des données.

Enfin, la conférence a abordé les questions de l'identification biométrique de l'individu. A cette occasion, nous avons présenté quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé (http://www.edsb.ch/f/doku/fachpresse/index.htm). L'utilisation de la biométrie n'est plus essentiellement réservée à des secteurs particuliers comme la poursuite ou la répression pénale. Elle se généralise et s'étend à de nombreuses applications dans le secteur public et dans le secteur privé. La biométrie ne se réduit pas à une technique, mais est d'abord une caractéristique propre de tout être vivant. Il existe une tendance à la banalisation de données relatives aux caractéristiques physiques et comportementales de la personne. La biométrie présente des risques non négligeables de violation des libertés et des droits et fondamentaux. La collecte et le traitement de données biométriques doivent intervenir dans le respect des exigences de protection des données et en particulier des principes de base (notamment licéité, bonne foi, finalité, proportionnalité, sécurité et droits des personnes concernées). La biométrie n'est pas la solution à tous nos problèmes de sécurisation des systèmes d'informations ou d'installations sensibles. Il faut rester prudent quant aux utilisations qui peuvent en être faites et quant au choix des technologies. Dans le secteur privé, l'utilisation de la biométrie comme moyen d'authentification est le plus souvent suffisant. On ne recourra à la biométrie que s'il n'y a pas d'autres moyens moins intrusifs d'atteindre l'objectif visé ou si elle est un élément de protection des données (voir également chiffre 2.2.2 du présent rapport d'activités).

Dans sa partie réservée aux commissaires à la protection des données, la conférence a adopté une résolution sur le projet de normes ISO de protection de la vie privée (http://26konferencja.giodo.gov.pl/rezolucje/j/fr/). L'organisation internationale de normalisation (ISO) prépare des normes internationales relatives aux principes de protection de la vie privée. Les commissaires à la protection des données sont favorables à cette initiative et souhaitent être associés activement à l'élaboration de celles-ci. Ces normes doivent avoir pour objectif de favoriser la mise en œuvre des obligations légales

en matière de protection des données et de la vie privée là où les obligations existent, et de les formuler là où elles font défaut. La conférence estime cependant que le projet de l'ISO ne permet pas d'atteindre cet objectif. En particulier, l'élaboration d'une norme internationale doit être fondée sur le principe de transparence («Fair Informations Practices»), ainsi que sur les principes de rareté, de minimisation et d'anonymisation des données. Pour être efficace, une telle norme doit:

- prévoir des critères d'analyse et d'évaluation concernant les fonctionnalités de protection de la vie privée de tout système ou technologie en vue d'aider les responsables de traitement à se conformer aux instruments juridiques de protection de données nationaux ou internationaux,
- fournir des garanties concernant les exigences en matière de protection de la vie privée au regard des technologies et des systèmes utilisés à des fins de gestion d'informations à caractère personnel,
- garantir les exigences de protection des données relatives aux personnes physiques, indépendamment du nombre d'organisations engagées dans le traitement et l'échange de ces données personnelles.

La 27ème Conférence internationale des commissaires à la protection des données aura lieu en Suisse à Montreux du 14 au 16 septembre 2005 (voir www.privacyconference2005.org). Intitulée «Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités», la conférence s'inscrit dans la ligne des conférences antérieures et devrait déboucher sur l'adoption d'une déclaration finale tendant à un renforcement du droit à la protection des données au plan universel.

9.4.2 Groupe de travail international pour la protection des données dans le domaine des télécommunications

Le PFPD a participé à la 24ème réunion du groupe de travail international pour la protection des données dans le domaine des télécommunications les 18 et 19 novembre 2004 à Berlin. Ce groupe a été créé en 1983 par les délégués à la protection des données de divers pays afin d'améliorer la protection des données dans le domaine des télécommunications et des médias.

En plus de l'échange mutuel d'informations sur les développements des législations des divers pays en matière de télécommunication, la réunion d'automne 2004 a notamment été consacrée aux moyens pour lutter contre la fraude sur Internet et qui sont compatibles avec la protection des données. Une poursuite pénale plus efficace et une meilleure collaboration entres les divers Etats est certes souhaitable, mais implique des collectes et des transferts de données pouvant être problématiques du point de vue de la protection des données. Le groupe de travail insiste sur les effets positifs des techniques préventives auxquelles on n'attache – en règle générale – pas encore assez d'importance. Il propose que les autorités prennent en considération des moyens respectant les principes de la protection des données, tels que la signature numérique, le recours aux services d'un tiers de confiance pour le commerce sur internet, les audits/labels de qualité, etc., avant de prendre des mesures affectant la sphère privée des individus. Les autorités devraient rassembler et échanger des informations sur de telles mesures et informer le public.

Un autre thème discuté a été celui des informations toujours plus précises que les services de téléphonie mobile peuvent recueillir sur la position géographique d'une personne. Cette possibilité conduit à l'offre de nouveaux services, notamment par des entreprises tierces qui ne sont pas soumises au secret des télécommunications. Du point de vue de la protection des données, le nombre de données personnelles traitées dans ce domaine doit être réduit au minimum. Une géolocalisation précise ne doit être activée que sur demande expresse et non par défaut. L'utilisateur doit en outre pouvoir décider lui-même dans quelle mesure des informations précises sur son emplacement peuvent être traitées. De plus, la communication de telles données doit être assujettie à l'accord de la personne concernée.

Parmi les autres thèmes discutés, citons les techniques radios à courte portée (communication directe entre deux appareils sans opérateur intermédiaire – p.ex. liaison Bluetooth entre une oreillette et un téléphone portable), les installations de surveillance vidéo qui enregistrent les comportements hors norme ainsi que la conservation de données de télécommunication à des fins de poursuite pénale.

Les documents (en allemand et en anglais) qui ont été adoptés par le groupe de travail sont disponibles sur internet à l'adresse suivante: http://www.datenschutz-berlin.de/doc/int/iwgdpt/.

10 Le Préposé fédéral à la protection des données

10.1 Les publications du PFPD – Nouvelles parutions

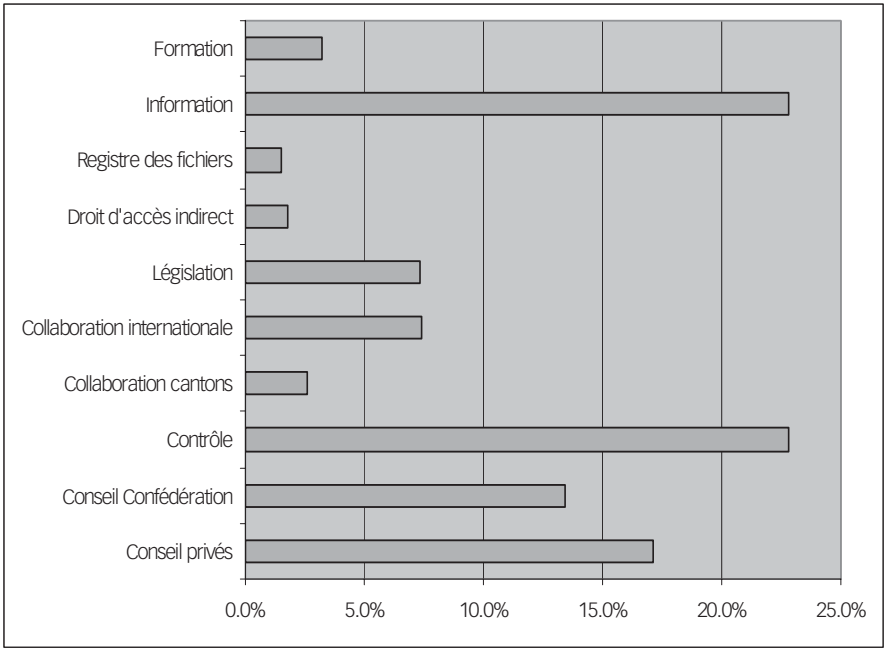
Par «spam» (ou «pourriel») il faut entendre un message électronique non sollicité, généralement indésirable et répété, envoyé en masse et ayant très souvent un caractère commercial. Les spécialistes préfèrent d'ailleurs parler d'UBE (Unsolicited Bulk E-Mails, ou courriels de masse non sollicités) et d'UCE (Unsolicited Commercial E-Mails, ou courriels commerciaux non sollicités). Les spams sont en grande majorité du type UCE mais ils peuvent apparaître dans bien d'autres contextes, lors des campagnes précédant une élection ou une votation, par exemple, ou pour diffuser des canulars. Il faut noter que les messages électroniques occasionnels d'une entreprise dont vous êtes client ne sont considérés comme spams, à condition toutefois que vous ayez donné votre accord pour ces envois.

Notre aide-mémoire concernant le spam explique les tenants et les aboutissants de la problématique du spamming et fournit des indications utiles pour lutter contre les spams et gérer les courriels non sollicités.

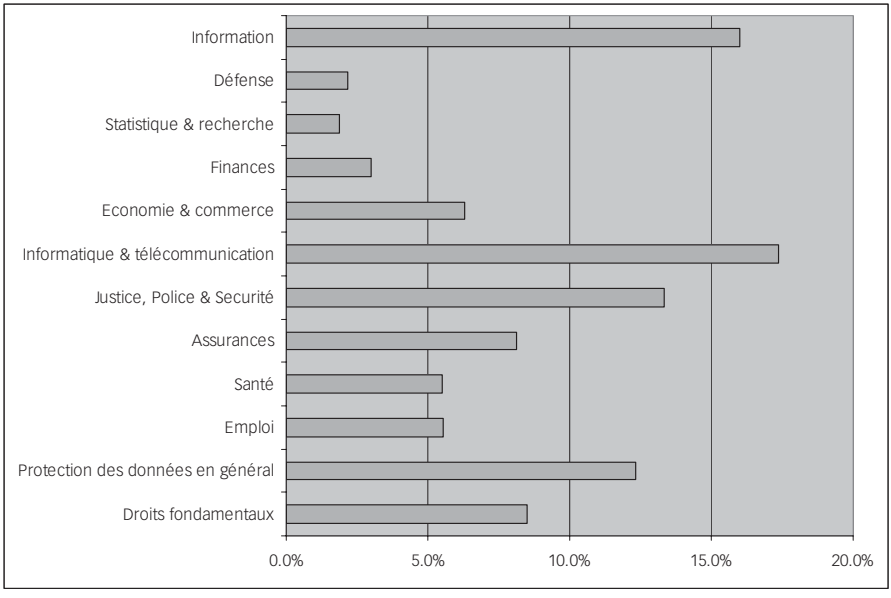
L'aide-mémoire se trouve dans l'annexe du présent rapport (chiffre 11.1) ainsi que sur notre site internet (http://www.edsb.ch/f/doku/merkblaetter/spam.htm).

10.2 Statistique des activités du Préposé fédéral à la protection des données. Période du 1er avril 2004 au 31 mars 2005

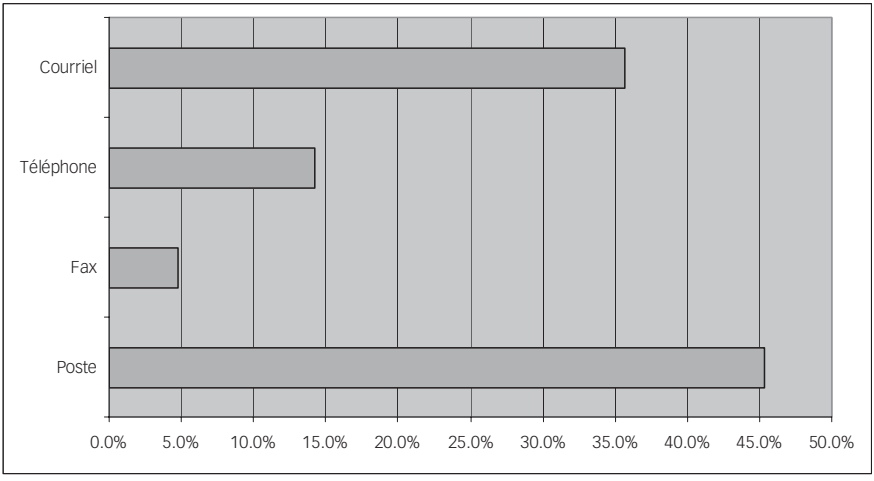
Charge de travail par tâches



Charge de travail par domaine



Provenance des demandes



10.3 Secrétariat du Préposé fédéral à la protection des données

Préposé fédéral à la protection des données:	Thür Hanspeter, Fürsprecher
Suppléant:	Walter Jean-Philippe, Dr. iur.
Secrétariat:	
Chef:	Walter Jean-Philippe, Dr. iur.
Suppléant:	Buntschu Marc, lic. iur.
Unité Conseil et Information:	8 personnes
Unité Surveillance:	9 personnes
Chancellerie:	3 personnes

11 Annexe

11.1 Aide-mémoire concernant les messages publicitaires indésirables diffusés par courrier électronique (spams)

Par «spam» (ou «pourriel») il faut entendre un message électronique non sollicité, généralement indésirable et répété, envoyé en masse et ayant très souvent un caractère commercial. Les spécialistes préfèrent d'ailleurs parler d'UBE (Unsolicited Bulk E-Mails, ou courriels de masse non sollicités) et d'UCE (Unsolicited Commercial E-Mails, ou courriels commerciaux non sollicités). Les spams sont en grande majorité du type UCE mais ils peuvent apparaître dans bien d'autres contextes, lors des campagnes précédant une élection ou une votation, par exemple, ou pour diffuser des canulars. Il faut noter que ni les messages électroniques occasionnels d'une entreprise dont vous êtes client, ni le bulletin d'information auquel vous vous êtes abonné ne sont considérés comme spams, à condition toutefois que vous ayez donné votre accord pour ces envois.

La présente notice explique les tenants et les aboutissants de la problématique du spamming et fournit des indications utiles pour lutter contre les spams et gérer les courriels non sollicités.

1. Collecte des adresses électroniques

Les expéditeurs de courrier électronique non sollicité (les «spammeurs») se procurent leurs adresses électroniques au moyen de puissants moteurs de recherche écumant les espaces et les forums publics d'Internet, ou encore en achetant des listes compilées par des tiers. Ils peuvent également créer leurs adresses en combinant des listes de noms et des noms de domaines particulièrement populaires. Une adresse électronique telle que peter.muster@domain.ch est ainsi plus vulnérable qu'une séquence aléatoire (p.ex. tr56&&@domain.ch). Les éditeurs de logiciels anti-virus estiment depuis peu qu'une collaboration entre spammeurs et créateurs de virus est vraisemblable, avec une tactique commune qui se présente à peu près comme suit: les auteurs de virus mettent en circulation des vers informatiques qui ouvrent une porte dérobée donnant accès aux ordinateurs personnels infectés; les spammeurs n'ont alors plus qu'à y pénétrer avec les moyens appropriés et à se servir de la messagerie de la victime pour expédier des spams à un nombre indéterminé de destinataires.

2. Conséquences pour les destinataires

Les spammeurs ne donnent à leurs destinataires aucune possibilité de mettre fin à leurs envois non sollicités. Dans la plupart des cas, l'adresse d'expéditeur qu'ils indiquent n'est pas valide, ce qui empêche toute demande de radiation de la part du destinataire. Les expéditeurs de spams recourent généralement à l'anonymat pour inonder les messageries d'offres commerciales douteuses. Or, les spams surchargent Internet, ils engendrent des frais de communication, font déborder les boîtes aux lettres électroniques et sollicitent les capacités de stockage des ordinateurs personnels touchés.

3. Spams et protection des données

3.1 Les adresses électroniques constituent des données personnelles permettant d'identifier une personne, dès lors que son nom y figure ou que l'adresse peut être associée à une personne précise. Dans ces conditions, le traitement d'adresses électroniques relève de la législation relative à la protection des données. Conformément à l'art. 12, al. 3, de la loi fédérale sur la protection des données (LPD, RS 235.1), il n'y a, en règle générale, pas d'atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement. Les données sont notamment présumées accessibles à tout un chacun lorsqu'une personne a publié son adresse électronique sur son propre site Internet. Or, même dans ce cas, on a le droit de refuser les envois publicitaires, et la non-observation de ce refus constitue une atteinte à la personnalité.

3. 2 Lorsqu'une adresse électronique n'est utilisée que dans un but spécifique (établissement de listes d'envoi, participation à des forums ou commande de marchandises sur Internet), elle n'est pas considérée comme accessible à tout un chacun au sens de l'art. 12, al. 3, LPD. Le traitement d'adresses électroniques de ce type par un spammeur constitue un détournement du but premier (art. 4, al. 3, LPD), commis à l'insu (art. 4, al. 2, LPD) et sans le consentement (art. 13, al. 1, LPD) de la personne concernée. Il s'agit donc bien d'une atteinte à la protection des données, mais si aucune information personnelle particulièrement digne de protection n'est traitée en même temps que l'adresse électronique, l'atteinte à la personnalité doit être qualifiée de peu importante. La loi sur la protection des données donne aux personnes concernées la possibilité d'agir en justice (art. 15 LPD; cf. également les art. 28 ss. du Code civil, CC, RS 210). Ces personnes peuvent notamment introduire une action en constatation de droit contre l'expéditeur

de spams. Elles peuvent également demander des dommages-intérêts et/ou une indemnité à titre de réparation morale. Il faut toutefois remarquer que l'atteinte à la personnalité est en règle générale de peu de gravité et que le dommage est en outre difficile à démontrer. Étant donné que le spammeur agit souvent sous le couvert de l'anonymat ou depuis l'étranger, la poursuite en justice se révèle très compliquée et implique la plupart du temps le recours (coûteux) à un avocat. Opter pour la voie judiciaire constitue le plus souvent une solution chère et compliquée.

3. 3 Si un spammeur cède ses fichiers d'adresses à un tiers, il doit signaler le fait au Préposé fédéral à la protection des données dès lors que la cession s'effectue à l'insu des personnes concernées (art. 11, al. 3, LPD).

4. Spams et probité commerciale

La branche de la publicité en Suisse s'est donné pour but de lutter contre la communication commerciale déloyale (dont notamment toutes les formes de publicité déloyale). À cet effet, elle a mis sur pied une commission (la Commission suisse pour la loyauté) composée à parts égales de consommateurs, de professionnels des médias et de publicitaires. Toute personne a le droit de dénoncer devant celle-ci, à titre gratuit, une publicité qu'elle estime déloyale. Les règles adoptées par la commission constituent des normes éthiques que la branche de la publicité s'est donnée elle-même. La commission fonde ses activités sur la législation suisse en matière de loyauté (cf. notamment la loi fédérale contre la concurrence déloyale, LCD, RS 241) et sur le Code correspondant de la Chambre de Commerce Internationale, dans sa portée internationale. La LCD prévoit que les personnes lésées peuvent intenter des actions en dommages-intérêts et en réparation du tort moral (art. 9, al. 3, LCD).

Conformément au point 4.4 des Règles de la Commission suisse pour la loyauté, les méthodes de vente à distance relèvent de la communication commerciale adressée personnellement à des individus. Cette définition englobe les spams. Les règles précisent en outre que les communications de ce type sont réputées agressives, donc déloyales, quand l'expéditeur omet d'offrir au destinataire la possibilité de déclarer, à l'aide du même moyen de communication, qu'il ne souhaite plus recevoir de communication commerciale (par exemple, par une option correspondante sur son site Internet ou sous la forme d'un lien actif «*unsubscribe*» permettant de faire cesser les envois). La solution proposée, qui charge les destinataires de manifester leur désir d'être radié de la liste d'envoi (**option de la radiation**, ou **solution de l'*opt-out***), autorise le spammeur à établir un premier contact par courrier électronique. Si le destinataire n'entend pas recevoir de courriels supplémentaires, il doit le faire savoir. Malheureusement, la plupart des spammeurs ne respectent pas cette décision. Bien

au contraire, en cliquant sur le lien «*unsubscribe*», le destinataire confirme qu'il a reçu le courriel et, par là-même, que l'adresse utilisée est valide. Autre aspect contestable: les spammeurs sont tenus d'établir des listes contenant précisément les adresses de toutes les personnes qui ne veulent rien avoir à faire avec eux.

5. Mesures législatives anti-spams en préparation

Deux lois fédérales sont en cours de révision. Il s'agit premièrement de compléter la loi sur les télécommunications (LTC, RS 784.10): les fournisseurs de services de télécommunication devront prendre des mesures appropriées et raisonnables pour empêcher la transmission de messages publicitaires à leurs clients qui ne seraient pas déjà en relation commerciale avec l'expéditeur ou qui n'auraient pas consenti explicitement à recevoir ces messages (art. 45*a* (nouveau) LTC).

Deuxièmement, la loi fédérale contre la concurrence déloyale devra être adaptée en conséquence. Le projet de révision prévoit que quiconque utilisera des moyens de télécommunication pour adresser des messages publicitaires à des personnes qui n'auraient pas donné leur consentement explicite ou avec lesquelles il ne serait pas déjà en relation commerciale aura agi de façon déloyale (art. 3, let. n (nouvelle), LCD). L'expéditeur devra donc s'assurer du consentement de ses clients avant même d'établir un premier contact commercial avec eux (**option de l'inscription**, ou **solution de l'*opt-in***).

6. Mesures techniques et organisationnelles contre les spams

Prenez vos précautions lorsque vous divulguez votre adresse électronique. Dès que celle-ci apparaît sur une page web (parce que vous avez participé à un forum de discussion, que vous vous êtes abonné à un bulletin d'information, que vous avez effectué des achats en ligne ou que vous avez rempli un formulaire, p.ex.), il se peut très bien qu'un tiers s'en empare à votre insu et sans votre consentement.

Les mesures préventives suivantes vous aideront à vous protéger de spams:

a. Choisissez soigneusement votre adresse électronique

évitez d'y faire figurer vos nom et prénom, les spammeurs auront ainsi plus de mal à la collecter.

b. Contrôlez l'usage qui sera fait de votre adresse sur Internet

avant de confier votre adresse électronique à un formulaire en ligne, assurez-vous que l'utilisation qui sera faite de votre adresse est bien spécifiée; vous pouvez ainsi réduire le risque de la voir transmise à des indésirables (à des fins de marketing, par exemple); vous devez en outre vous faire informer sur les destinataires subséquents de vos données ainsi que sur votre droit d'accès.

c. Utilisez plusieurs adresses électroniques

créez une adresse spécifique pour effectuer des transactions commerciales sur Internet, participer à des forums ou recevoir des bulletins d'information; vous pouvez ainsi protéger efficacement votre adresse électronique personnelle, que vous réserverez à vos contacts professionnels et personnels.

d. Dressez la liste des destinataires de vos courriels

vous avez intérêt à imprimer et à conserver les données (date d'inscription, contenu du courriel, mot de passe) que vous fournissez lorsque vous vous abonnez à un bulletin d'information, lorsque vous ouvrez un compte ou lorsque vous effectuez un paiement en ligne; il n'est pas impossible, par exemple, qu'un bulletin d'information fictif serve de couverture à un spammeur; vous devriez de même établir la liste des sites web sur lesquels vous avez publié votre adresse électronique.

e. Protégez les adresses électroniques de tiers

lorsque vous envoyez un message à plusieurs destinataires, servez-vous de la zone «copie invisible» (Cci, copie carbone invisible; en anglais, Bcc, Blind carbon copy) de votre logiciel de messagerie: vous protégez ainsi l'adresse de vos correspondants; dissimulez également ces adresses lorsque vous participez à un forum, ainsi que sur les listes d'envoi.

f. Obtenez d'abord le consentement des personnes concernées

ne révélez jamais l'adresse d'un tiers sans son consentement.

g. Utilisez un filtre anti-spams

il est aujourd'hui possible de s'attaquer au problème des spams en recourant à des analyses de contenu ou d'en-têtes; les courriels reçus sont analysés et filtrés en fonction de certaines caractéristiques, même si cette approche ne résout pas tous les problèmes; d'une part en effet, il arrive que des messages parfaitement légitimes soient retenus par le filtre: en règle générale, il faut compter avec un taux d'erreur d'au moins 10% (faux positifs et faux négatifs); d'autre part le vrai problème n'est pas résolu: les spams n'en sont pas moins expédiés, le filtre ne fait que vous épargner un

peu de travail; il faut noter que les fournisseurs d'accès à Internet sont de plus en plus nombreux à offrir leur propre filtre anti-spams, qui passe en revue les boîtes postales directement sur le serveur d'hébergement; si votre fournisseur propose ce service, vous pouvez gérer vous-même le filtre anti-spams au niveau de votre compte de messagerie; ce faisant, vous pouvez choisir si les courriels reconnus comme spams doivent être effacés sans intervention de votre part dès leur réception sur le serveur, ou s'ils doivent être déplacés dans un dossier réservé aux spams.

h. Annoncez la couleur dans les annuaires publics

dans la mesure du possible, précisez (dans un annuaire téléphonique électronique, par exemple) que vous ne désirez pas recevoir de publicité non sollicitée.

i. Pensez à vous faire inscrire sur des listes de blocage

l'efficacité de ces listes, qui vous permettent de signaler que vous ne désirez pas recevoir de messages non sollicités, dépend toutefois de la bonne volonté des spammeurs; vous risquez également que l'inscription sur une liste de blocage soit interprétée comme une confirmation de la validité de votre adresse électronique et qu'un spammeur en fasse un usage abusif.

j. Ne négligez pas les listes noires

les fournisseurs de services de messagerie électronique sont à même de contrôler, à l'aide de listes noires, si le serveur d'où est parti un message est connu pour diffuser des spams; le cas échéant, le message peut être refusé; au moment de choisir votre fournisseur, vous devriez vous assurer qu'il dispose effectivement d'une liste de ce type.

Lorsque vous recevez un courrier électronique non sollicité, appliquez les règles suivantes:

a. Supprimez le message sans le lire

la meilleure solution consiste à supprimer les spams sans les ouvrir; n'ouvrez en aucun cas les pièces jointes et n'acceptez aucune offre commerciale, aussi alléchant que puisse paraître le courriel publicitaire.

b. Ne répondez pas aux spams

veillez à ne jamais répondre à un spam; toute réponse confirme au spammeur que votre adresse est valide et qu'elle est utilisée; le spammeur peut ainsi continuer à vous envoyer des courriels non sollicités et il peut même revendre votre adresse à des tiers; vous ne devriez répondre à un courriel non sollicité que s'il offre la possibilité de faire radier votre adresse (*opt-out*) ou lorsque vous disposez d'une adresse électronique spécifiquement créée pour ce type de courriels.

c. Évitez toute réaction excessive

ne cherchez pas inonder la boîte aux lettres électronique du spammeur avec de gros volumes de données; il se pourrait en effet que le spammeur ait eu recours à une fausse signature: soit que l'adresse fournie n'existe tout simplement pas, soit qu'elle appartienne à une autre victime du spammeur; en outre, vous ne feriez que surcharger inutilement Internet à votre tour.

d. Ne cliquez jamais sur les liens hypertextes des spams

en cliquant sur ces liens, vous risquez de voir un spammeur capter votre adresse électronique, par exemple au moyen d'un témoin de connexion (ou *cookie*), ce qui lui fournira la confirmation que votre adresse est effectivement utilisée.

e. Informez les fournisseurs d'accès Internet ou de services de messagerie

informez le propriétaire du serveur de messagerie utilisé par le spammeur ou votre propre fournisseur d'accès Internet; la plupart des fournisseurs d'accès ou de services de messagerie ont créé des boîtes aux lettres électroniques destinées à cet usage; ils sont à même d'agir contre les spammeurs et de mieux protéger les utilisateurs contre les messages électroniques non sollicités.

f. Recourez aux logiciels spécialisés

des logiciels spécifiques vous permettent de contrôler le contenu de votre boîte aux lettres directement sur le serveur d'hébergement; ils affichent les expéditeurs, la rubrique «Objet» correspondante et la taille du message; vous pouvez ainsi supprimer les messages indésirables en quelques clicks de souris avant de télécharger le reste de votre boîte aux lettres à l'aide de votre logiciel de messagerie usuel.

g. Dénoncez les menaces dont vous faites l'objet

lorsqu'un spammeur vous menace (par exemple de diffuser sous votre nom des messages à contenu pornographique), déposez plainte auprès des autorités pénales compétentes.

7. Liens

Les organisations suivantes, officielles, internationales ou privées, abordent le thème du courrier électronique non sollicité:

- http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/communic_reports/spam/spam_com_2004_28_fr.pdf
- http://cm.coe.int/ta/rec/1995/f95r4.htm
- http://cm.coe.int/ta/rec/1999/f99r5.htm
- http://www.oecd.org/dataoecd/55/32/31450810.pdf
- http://www2.dcita.gov.au/ie/trust/improving/spam_home
- http://www.cnil.fr/index.php?id=1266
- http://www.datenschutz-berlin.de/jahresbe/03/teil3.htm#3
- http://spamlaws.com
- http://www.siug.ch/positionen/SIUG-Spam.shtml
- http://www.euro.cauce.org
- http://spamcop.net
- http://www.sncd.org/deontologie/index.html
- http://www.imc.org/imc-spam/index.html
- http://spamanti.net
- http://www.caspam.org
- http://www.lauterkeit.ch/pdf/grundsaetze.pdf